



HM TREASURY

Internal Audit Records Management

June 2011



HM TREASURY

Internal Audit Records Management

June 2011



Official versions of this document are printed on 100% recycled paper. When you have finished with it please recycle it again.

If using an electronic version of the document, please consider the environment and only print the pages which you need and recycle them when you have finished.

© Crown copyright 2011

You may re-use this information (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view this licence, visit <http://www.nationalarchives.gov.uk/doc/open-government-licence/> or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or e-mail: psi@nationalarchives.gsi.gov.uk.

ISBN 978-1-84532-889-4
PU1194

Contents

		Page
Chapter 1	Introduction	3
Chapter 2	HIA Policy	5
Chapter 3	Aims and Objectives	7
Chapter 4	Responsibilities for managing Information	9
Chapter 5	Information Security	11
Chapter 6	Record Organisation	13
Chapter 7	Retention and Disposal	15
Chapter 8	Handling Requests for Information	19
Annex A	Retention Schedule	23
Annex B	Legislation and Regulations	25

1

Introduction

1.1 This guide has been produced for all government organisations that are required to comply with the Government Internal Audit Standards (GIAS)¹ 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 Public Records Act² guidance produced by National Archives, the Information Commissioner’s Office and the Ministry of Justice (MOJ).

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 Government Internal Audit Standards state that the HIA “must develop retention requirements consistent with the organisation’s guidelines and any pertinent regulatory or other requirements” (2330.A2).

1.3 A record³ 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; and
- demonstrate compliance with standards for the professional practice of internal auditing and with relevant legislation and regulations.

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

¹ Standard 2330 covers Documenting Information to support the conclusions and engagement results.

² www.nationalarchives.gov.uk/poly/act/default.htm

³ ISO 15489 definition of a record.

2

HIA Policy

2.1 The Head of Internal Audit (HIA) should establish and communicate a clear policy for the management of information to all internal audit staff. The policy, which should be consistent with the organisation's records management policy, 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 (e.g. under the Freedom of Information Act or the Data Protection Act) (**Section 8**);
- Outline appropriate legislation and regulations relevant to the environment in which the internal audit service operates (**Annex B**).

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 HIA has overall responsibility for ensuring that information is managed responsibly by the internal audit service (see GIAS 2330 on documenting information). Everybody in the audit service has a role to play in ensuring that information is complete, up to date and protected against loss and unauthorised access. The HIA might typically provide regular assurance to the organisation's Senior Information Risk Owner (SIRO) 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 service, 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 HIA 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 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, even by home workers, are corporate 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 or remote working policy;
- 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 home or remote working policies.

5

Information Security

Standards

5.1 The Standards state that the Head of Internal Audit (HIA) must control access to engagement records. The HIA 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. Information assurance guidance can be found on the CESG website.¹ Also relevant is the HMG Security Policy Framework² that sets mandatory measures in 7 key security areas including information security.

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 GIAS and does not place the organisation in potential breach of relevant regulations.

¹ http://www.cesg.gov.uk/products_services/iacs/index.shtml

² http://www.cabinetoffice.gov.uk/media/207318/hmg_security_policy.pdf

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 HIA 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 Records should include good metadata (information to help identify records). The e-Government Metadata Standard (e-GMS)¹ lays down the elements, refinements and encoding schemes to be used by government officers when creating metadata for their information resources or when designing search systems for information systems. However, commonsense, good naming conventions and filing structures can help to support efficient retrieval.

¹ See <http://interim.cabinetoffice.gov.uk/govtalk/schemasstandards/metadata.aspx>

7

Retention and Disposal

7.1 The Standards state that the HIA 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 HIAs should develop an information retention and disposal policy that is consistent with the organisation's guidelines and any relevant regulations or legislation. Some internal audit information may need to be kept for up to 6 years in accordance with the Limitation Act 1980. Retention schedules should define a retention period for each type of record which 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). An example of a records retention schedule is provided at [Appendix A](#).

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 HIA 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.

7.8 The Data Protection Act 1998 may affect the retention of information. The Act does not specify how long information may or must be retained but organisations are required to set down their policies on retention. Internal Audit information must be kept for as long as the policies state. Principle 5 of the Data Protection Act 1998 states that personal information “shall not be kept for longer than is necessary for that purpose or those purposes”.

7.9 National Archives Guidelines states that information collected as part of a fraud investigation should be kept for 6 years after legal proceedings have been completed.

7.10 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. Government 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 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.
- 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. Government 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. NAO want to see them; 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.
- Historic purposes. National Archives guidance states that “it is unlikely that many records relating to internal audit will be selected for permanent preservation. Criteria for selecting records for historical purposes can be found in the publication Acquisition and Disposition Policies (PRO 2000) and in more detailed operational selection policies. No records should be destroyed without reference to those documents and all internal audit records no longer required for business purposes should be subject to the formal appraisal process to determine whether they fall within the criteria of selection for permanent preservation”.

7.11 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.

7.12 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.

External Service Providers/Shared Services/Third Party Assurance

7.13 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 organisation 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.

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

7.15 Where Heads of Internal Audit seek assurance from other assurance providers in their organisations (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 service requires.

8

Handling Requests for Information

Introduction

8.1 Requests for information should be dealt with in accordance with relevant laws, and regulations (see Appendix B) and the organisation's information sharing policies. The main legal acts under which information might be requested include:

- **The Freedom of Information Act 2000.** This Act gives the general public access to information on how government bodies make decisions and run services. It sets out strict timetables for compliance with a request for information, states that the costs of retrieving information must be reasonable and asserts that all recorded information held, wherever it is located, is potentially disclosable. Guidance is available from Ministry of Justice¹ including guidance about exemptions² particularly Section 33 on Audit Functions³. The National Archives website⁴ is another useful source of information as is the Information Commissioner's website⁵. Other useful guides about dealing with requests for information are available on the Ministry of Justice website⁶.
- **The Data Protection Act 1998.** The Act gives individuals the right to access information about them that is held by organisations. An explanation of the Data Protection Act is contained in the National Archives publication "Data Protection Act 1998: A Guide for Records Managers and Archivists"⁷. Internal auditors may hold personal information as a result of reviews of areas involving personal information such as payroll, travel and subsistence or human resources.
- **The Environmental Information Regulations 2004⁸** (EIR) give rights of public access to environmental information held by public authorities. It is important for public authorities to identify environmental information correctly in order to deal with information request. To deal with requests, it is important to understand the distinction between:
 - Environmental information, which would fall within the scope of the EIR;
 - Personal data of the requester, which falls under the Data Protection Act 1998; and
 - All other information, which falls under the FOIA.

¹ <http://www.justice.gov.uk/guidance/guidancefoi.htm>

² <http://www.justice.gov.uk/guidance/foi-exemptions.htm>

³ <http://www.justice.gov.uk/docs/foi-exemption-s33.pdf>

⁴ <http://www.nationalarchives.gov.uk/policy/foi/>

⁵ <http://www.ico.gov.uk/>

⁶ <http://www.justice.gov.uk/guidance/foi-guidance-codes-practice.htm>

⁷ <http://www.nationalarchives.gov.uk/documents/information-management/dpguide.pdf>

⁸ http://www.ico.gov.uk/upload/documents/library/environmental_info_reg/introductory/eir_what_is_environmental_information.pdf

Requests for Information Under the Freedom of Information Act

8.2 Most requests for information are likely to arise under the Freedom of Information Act. The following guidance is based on advice offered by Ministry of Justice in their guide entitled "Freedom of Information Worked Example – Internal Audit Information". Guidance on exemptions can be found on the Ministry of Justice website.⁹

Assignment Information

8.3 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 HIA 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?

8.4 The main applicable exemption in relation to the internal audit process is s36(2)(c) – prejudice to effective conduct of public affairs. In addition s36(2)(b)(i) and s36(2)(b)(ii) which provide respectively that information is exempt if disclosure would inhibit the free and frank provision of advice and the free and frank exchange of views for the purposes of deliberation, may also apply.

8.5 Departments will need to consider whether disclosure under s36 would prejudice the internal audit process, following which, the public interest for and against disclosure must be considered.

8.6 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). Premature disclosure of audit information would be likely to be prejudicial to the conduct of public affairs and the exemptions at section 36(2)(b) i and ii and 36(2)(c) are likely to be engaged.

8.7 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.

8.8 As for all requests where a qualified exemption is engaged, the public interest arguments for and against disclosure will have to be considered.

8.9 Depending on the area being audited, the application of s36 may well be in combination with other exemptions (e.g. internal audit of a policy area may engage s35, internal audit of agencies with law enforcement duties may engage s30 or s31, internal audit of the implementation of an IT project or new procurement plan may engage s43).

Interim and Annual Reports

8.10 As interim and annual reports are part of the internal audit process s36(2)(c) will apply alongside subject based exemptions depending on the content of reports. Public interest

⁹ <http://www.justice.gov.uk/guidance/foi-exemptions-guidance.htm>

considerations also apply. In addition, these reports contain evaluations of the adequacy and effectiveness of risk management as well as disclosing internal control weaknesses. Again s36(2)(b) i and ii and s36(2)(c) could be applicable as disclosure could undermine the quality of reporting.

8.11 The passage of time is also an important consideration with the public interest in non-disclosure of these reports.

A

Retention Schedule

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 following schedule 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). More guidance is available from National Archives¹.

Item	Description	Minimum Retention Period	Maximum retention Period
Reports			
1.	Audit reports (including interim) where these have included 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 been completed	6 years after legal proceedings have been completed
3.	Annual Reports and information supporting the SIC/governance statement	1 year	3 years
4.	Other audit reports (including interim).	1 year	3 years
Undertakings			
5.	Terms of reference.	On completion of reviews (i.e. when all agreed actions have been implemented by management).	3 years
6.	Programmes/plans/strategies	As soon as they have been replaced by a new programme/plan/strategy.	1 year after the last date of the

¹ http://www.nationalarchives.gov.uk/documents/information-management/sched_internal_audit.pdf

Item	Description	Minimum Retention Period	Maximum retention Period
			plan
7.	Correspondence	Correspondence relating to reviews should be reviewed at the same time as other working papers (see below). Other correspondence should be reviewed after 6 months.	3 years
8.	Minutes of meetings and related papers.	1 year	3 years
9.	Working papers.	On completion of reviews (i.e. when all agreed actions have been implemented by management)	3 years
Other Information			
10.	Internal audit guides.	When superseded.	When superseded.
11.	Manuals and guides relating to departmental procedures.	When superseded.	When superseded.
12.	Local auditing standards	When superseded.	When superseded.

B

Legislation and Regulations

These include:

- **The Freedom of Information Act 2000** that covers all information that does not relate to the environment. It is intended to allow the public access to information on how government bodies make decisions and run services;
- **The Environmental Information Regulations 2004 (EIR)** which gives rights of public access to environmental information held by public authorities;
- **Lord Chancellor's Code of Practice** on the Management of Records under Section 46 of the Freedom of Information Act;
- **The Data Protection Act 1998** that was designed to prevent misuse of personal information. The Act gives individuals the right to access information about them that is held by organisations. It has implications for all aspects of records creation, maintenance, processing and disposal. The DPA means that:
 - You have to manage and process personal information properly;
 - The individual's right to privacy must be protected;
 - The individual has the right to access all personal information held about him/her.
- **Human Rights Act 1998** also covers access to information held about individuals.
- **ISO 15489** – International Standard on Records Management
- **ISO27701 and ISO27002** – Code of Practice on Information Security.
- **Public Records Acts 1958 and 1967** relating to the selection of records for permanent preservation and transfer to the National Archive.
- **Computer Misuse Act 1990** – the provisions of this Act are aimed at securing computer material against unauthorised access or modification.
- **Limitation Act 1980** – sets time limits within which different types of legal proceedings can be commenced (e.g. time limits within which a creditor can chase a debtor for outstanding debt). The Act recommends retention periods for certain types of record including some financial records, contracts, and personnel records.
- **The HMG Security Policy Framework**¹ which outlines the mandatory protective security requirements (including physical, information and personal security) that all Government Departments and Agencies must follow.
- **National Audit Act 1983** – for the purpose of carrying out value-for-money studies, section 8 of the Act provides the C&AG with a statutory right of access at all reasonable times to all such documents as may reasonably be required, provided that the documents are held by or under the control of the department or body concerned.

¹ http://www.cabinetoffice.gov.uk/media/207318/hmg_security_policy.pdf

HM Treasury contacts

This document can be found in full on our website at:
hm-treasury.gov.uk

If you require this information in another language, format or have general enquiries about HM Treasury and its work, contact:

Correspondence Team
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

Tel: 020 7270 4558

Fax: 020 7270 4861

E-mail: public.enquiries@hm-treasury.gov.uk

ISBN 978-1-84532-889-4



9 781845 328894 >