

GOODS AND SERVICES TAX

KEEPING OF RECORDS IN IMAGING SYSTEM



INLAND REVENUE
AUTHORITY
OF SINGAPORE

Keeping records in imaging system

Published by
Inland Revenue Authority of Singapore

Published on 18 November 2003
Revised on 1 July 2007

© 2007 IRAS Singapore. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording without the written permission of the copyright holder, application for which should be addressed to the publisher. Such written permission must also be obtained before any part of this publication is stored in a retrieval system of any nature.

TABLE OF CONTENTS

1 INTRODUCTION..... 1

2 Definition of Terms Used..... 1

3 Compliance Criteria 2

 3.1 Document Capture -- Image Quality 2

 3.2 Document Capture -- Image Enhancement..... 3

 3.3 Document Capture -- Image Editing..... 3

 3.4 Document Capture -- Image Indexing 4

 3.5 Document Capture -- Partial Image Capture..... 4

 3.6 Document Capture – Committal..... 4

 3.7 Document Capture – Completeness 5

 3.8 Document Capture – Additions 5

 3.9 Image Storage and Management -- Image Integrity..... 5

 3.10 Image Storage and Management -- Image Update..... 6

 3.11 Image Storage and Management -- Image Index Update 6

 3.12 Image Output -- Image Integrity 7

 3.13 Image Output -- Image Completeness 7

 3.14 Image Output -- Changed Images..... 7

 3.15 Image Output -- Composite Images 7

 3.16 Computer Applications..... 8

 3.17 Physical and Environmental Security..... 8

 3.18 System and Application Security..... 8

 3.19 Independent Record Keeper 8

4 Retention of Original Paper Documents..... 9

5 Penalties for Non-Compliance 9

6 Storage Media & File Format for Tax Audit Purposes 9

1 INTRODUCTION

Under the Income Tax Act and the Goods and Services Tax ('GST') Act, persons liable to pay income tax and GST registered businesses (referred to as "taxpayers") are required to keep their business records for a period of at least seven years, for records pertaining to prescribed accounting periods ending before 1 January 2007. The corresponding record-keeping duration is 5 years for records pertaining to prescribed accounting periods ending on or after 1 January 2007.

For Income Tax purposes, the records keeping requirements relate to the keeping of records which will enable the taxpayer's income and allowable deductions to be readily ascertained. For GST purposes, record keeping requirements include the keeping of business and accounting records, tax invoices and receipts issued, tax invoices received, import and export documentation, credit notes and debit notes.

The Evidence Act (Chapter 97) and the Evidence (Computer Output) Regulations 1996 provide that computer output and records may be admissible as evidence if the computer output and records are produced in a process which comply with criteria set out in the First Schedule to the Evidence (Computer Output) Regulations 1996.

Taxpayers do not need to seek approval from the Comptroller of Income Tax and GST to keep business records in an image system. A taxpayer may wish to have his image process approved as an approved process under the Evidence Act. However, if he decides not to obtain approval as an approved process under the Evidence Act, he can still store the business records in an image system provided that the image storage of business records will be carried out in accordance with the criteria set out in the First schedule to the Evidence (Computer Output) Regulations 1996.

This guide lists the compliance criteria set out in the First Schedule to the Evidence (Computer Output) Regulations 1996. Guidance on how these compliance criteria can be satisfied are also listed.

Where a taxpayer engages a service bureau to image, store and maintain the business records, he would still be required to ensure that the compliance criteria as set out in this guide are complied with.

2 Definition of Terms Used

In this Guide, the terms used, as defined under the First Schedule to the Evidence (Computer Output) Regulations 1996, are as follows:

- (a) **"approved process"** means a process that has been approved in accordance with The Evidence (Computer Output) Regulations 1996 by a certifying authority;

Keeping records in imaging system

- (b) **“audit trail”** means a computer record of changes to either the data enabling access to images or to the images themselves, where such changes affect the content or availability of images;
- (c) **“capture”** means the recording of the contents of a document by photographic, electronic or other means;
- (d) **“certification”** means the process of ensuring that a process constitutes an approved process for document reproduction in accordance with the compliance criteria;
- (e) **“certifying authority”** means a person or an organisation appointed by the Minister for Law to be a certifying authority in accordance with The Evidence (Computer Output) Regulations 1996;
- (f) **“committal”** means the introduction of a captured image into the database environment of the image system;
- (g) **“image”** means a representation of a document generated by photographic, electronic or other means, which is stored in the image system;
- (h) **“image system”** means any computer system that is capable of capturing, storing and retrieving images or generating image system output;
- (i) **“image system output”** means a computer output from an image system;
- (j) **“process”** includes a computer system.

3 Compliance Criteria

3.1 Document Capture -- Image Quality

All information contained in the document (be it graphical, textual, hand written or otherwise) must be capable of being captured in its entirety (except guidelines printed in drop-out ink for image recognition of data) and with a level of accuracy that ensures that no information that can reasonably be expected to form part of any subsequent business process is lost or altered in any way. Quality assurance procedures consistent with document volumes, the quality of the original documents or any other relevant factor, must be put into place to ensure image quality.

- (a) The scanning system used must include proven hardware and software components reputable for both quality and performance.
- (b) Provision must be made for the scanner operator to routinely check the quality of the images against a set of “benchmark” images and, if

Keeping records in imaging system

necessary, make adjustments to the scanner settings so as to ensure accurate and clear capturing of the contents of the document.

- (c) Where the volume of documents to be captured is large, a trained quality control staff should be engaged to conduct random checking of the image quality.

3.2 Document Capture -- Image Enhancement

Any technique of image enhancement must be very closely examined by the certifying authority. Where there is any doubt that the accuracy of the relevant contents of the original document may be affected by the enhancement technique, then an original, un-enhanced version of the image must be retained.

- (a) Enhancement tools should be used only for the removal of unwanted elements introduced by the scanning process or for improving the quality or clarity of the image.
- (b) Control procedures must be in place to prevent loss or corruption of the original contents of the document during the enhancement process.
- (c) Where an image has been substantially enhanced, the original unenhanced version of the image must be retained. If the original unenhanced image is of such poor quality as to be illegible, the original copy of the document must be kept.

3.3 Document Capture -- Image Editing

The image system must not allow erroneous alterations to be made to the image of an original document, whether through the editing of an image, the introduction of new images from another source or the deletion of one or more images. Where image editing forms a part of the normal business process prior to committal, a full audit trail must be maintained. Where there is any doubt that the accuracy of the relevant contents of the original document may be affected by the editing, then, an original un-edited version of the image must be retained.

- (a) Controls must be in place to prevent loss of information during editing.
- (b) Full audit trail of any editing made must be maintained.
- (c) An un-edited version of the image must be retained if the editing could result in the impairment of the original contents of the document.

Keeping records in imaging system

- (d) The original copy of the document must be retained if the information contained in the original document could not be properly captured even after editing.

3.4 Document Capture -- Image Indexing

Where information is required to be assigned to individual images or groups of images in order to facilitate future retrievals, reasonable steps must be taken to ensure that such information is accurate.

- (a) Staff who are involved in classifying and indexing captured documents must be properly trained.
- (b) There must be adequate checks or validating procedures to ensure that image indexing, be it manual or automated, is accurate.
- (c) Index values should, as far as possible, be automatically assigned by the system rather than typed in manually.
- (d) The index data must be stored in a secured environment to prevent accidental or deliberate data modification.

3.5 Document Capture -- Partial Image Capture

Where partial images are captured by the image system for efficiency reasons (e.g. only the data on a standard form, omitting background elements such as pre-printed logos, instructions, lines, shading, etc.) then the process must be capable of maintaining a record of the separate image elements of a document and their relationships.

- (a) The image of an oversized document must not be cropped when an image of it is being captured. However, images of the separate components of the oversized document can be captured if the relationship between the separate components can be maintained. If the relationship between the separate elements cannot be maintained, the original copy of the oversized document must be kept.
- (b) Where certain standard elements of a document are “dropped-out”, a separate record of these image elements which are “dropped-out” must be kept and properly related to each other so as to allow for subsequent reconstruction of the document if required.

3.6 Document Capture – Committal

The process must ensure that all valid images that are captured are correctly committed to the imaging system.

Keeping records in imaging system

- (a) Sufficient indexing detail must be assigned to the image in transitional storage for the identification and retrieval of the image prior to committal. Upon successful committal, full indexing must be done.
- (b) Once an image is committed, it should be placed in a secured environment with adequate disaster recovery procedures. This also applies to those images pending committal.

3.7 Document Capture – Completeness

The person or organisation seeking certification must put in place measures to ensure that all documents are captured in the event of a system disruption.

- (a) Measures to ensure completeness of information must be instituted throughout the whole imaging process from document preparation for scanning to final committal to the database.
- (b) In the event of system failure or disruption at any stage of the imaging process, there should be adequate controls or recovery procedures to ensure that information contained in the original document is not lost.

3.8 Document Capture – Additions

Where, as part of a business process, information is added to a document or an image thereof (either physically or electronically) and the original information and the new information must be distinguished for the life of the document or the image thereof, then, the new information must be clearly distinguishable from the original information. This may be achieved by the content or context of the new information, its placement, colour (in the case of colour imaging) or any other relevant method.

- (a) Where information needs to be added on to the original document prior to scanning, provisions should be made for the clear distinguishing of the original contents of the document from the information that has been added.
- (b) Due care must be exercised when inserting the additional information to ensure that the integrity and accuracy of the original document are not impaired.

3.9 Image Storage and Management -- Image Integrity

From the time that committal of an image commences until the time that an image is no longer required to be retained, the image system must ensure that the image and any other data associated with that image can be

Keeping records in imaging system

retrieved. Therefore, reasonable image and data security, backup and recovery measures must be in place.

- (a) The system must be able to reproduce the complete information from all the separate components associated with an image.
- (b) All images and their associated information and index data must be properly backed up for subsequent recovery in the event of system failure or disruption.
- (c) When changing storage media, proper measures must be taken to ensure that index data and images are not lost or corrupted.

3.10 Image Storage and Management -- Image Update

The image system must not allow changes to be made to the images after the committal of that image.

- (a) Image update through the deletion of the image after committal is strictly prohibited.
- (b) If changes are required to be made to the contents of an image, it should only be done through the use of a separate edit layer and not directly onto the image itself. The edit layer must also be capable of being clearly distinguishable from the original copy of the image and be retrievable separately.
- (c) A full audit trail should be kept of all image updates.

3.11 Image Storage and Management -- Image Index Update

In the event of a change to the image index which may affect the retrieval of the images, a full audit trail must be maintained and a previous unamended version of the image or group of images should be retained.

- (a) Proper control measures must be taken when performing an index update. Measures taken could include having a senior or properly trained staff to perform the update and a separate officer to verify it.
- (b) A full audit trail must be kept of all updates made to the image indices. A previous unamended version of the image prior to the index update should be kept for subsequent retracing if required.
- (c) In the event that a system generated audit trail is not available due to the use of special access facilities, a manual audit trail record should be maintained. The use of such special access privileges should be restricted and properly controlled.

Keeping records in imaging system

3.12 Image Output -- Image Integrity

Reasonable measures must be in place to ensure that, once output by the image system (i.e. when the image is no longer under the control of the image system database environment), the images cannot be tampered with (e.g. in the case of printed output, the print spool must be secured).

- (a) When an image and its related data are placed in a transitional environment pending output, the transitional environment must be properly secured to prevent tampering of the contents of the image and the related data.

3.13 Image Output -- Image Completeness

Where data has been captured during the life of the image, which may reasonably be expected to form a part of the information relating to that document (e.g. annotations, notes, overlays, etc.) then the image system must be capable of accurately reproducing that information together with the output images.

- (a) The system must be capable of printing and displaying or indicating all the information that is associated with the image.

3.14 Image Output -- Changed Images

Where an image or group of images have been amended or erroneously tampered with, the system must be capable of producing an audit trail together with the image system output.

- (a) The system must be able to indicate that amendments or updates have been made to an image during image output.
- (b) The audit trails of changes made to the index data or images must be capable of being printed for subsequent verification.

3.15 Image Output -- Composite Images

Where an image system output is generated as a result of the combination of two or more separate images (through techniques such as overlaying) particularly when one or more of these separate images were not directly generated from the original document, then adequate procedures must be in place to ensure that the combined output accurately represents the original document.

- (a) When combining images for output, due care must be taken to ensure that the original contents of the respective images is not impaired.

Keeping records in imaging system

3.16 Computer Applications

Where computer applications or programs are developed to automate any of the document capture, storage and management or output procedures, they must not contravene any of the compliance criteria specified in the First Schedule of the Evidence Act.

- (a) All programs or computer applications, whether directly or indirectly linked to the image system, must comply strictly with all the provisions of the First Schedule.
- (b) There should be in place a general control framework to provide a reasonable assurance that the whole image process is conducted within a secured environment.
- (c) Images must remain retrievable in the event of system change, computer upgrades or change of software or hardware vendors.

3.17 Physical and Environmental Security

Reasonable physical and environmental measures must be in place to protect the equipment and storage media from unauthorised access and excessive environmental levels.

- (a) Adequate physical and environment security measures should be taken to prevent the risk of accidental or malicious damage to, or theft of computer equipment or media.
- (b) Routine checks should be made of media and backup copies of files to prevent the loss of data through media deterioration.

3.18 System and Application Security

Security controls must be implemented to prevent unauthorised access and modifications to the image file, the index file containing descriptive information about the image file as well as the audit trail. Physical security of the data including backup and recovery must be addressed.

- (a) Image file, index file containing descriptive information about the image file and the audit trail log should be secured with appropriate logical access control measures and physical controls to prevent unauthorised access and modifications.

3.19 Independent Record Keeper

Where a private organisation chooses to have a copy of each image kept by an independent record keeper for the purpose of complying with the relevant criteria relating to security, integrity and back-up of images, the

Keeping records in imaging system

organisation must ensure that the copy of each image kept by the record keeper is complete, accurate and retrievable.

4 Retention of Original Paper Documents

The original copies of the documents must be kept unless the image storage of the business records has been carried out in accordance with the requirements set out in this guide.

5 Penalties for Non-Compliance

Failure to comply with the criteria set out in this guide may constitute an offence under section 67 read with section 94 of the Income Tax Act or an offence under section 46(6) of the Goods and Services Tax Act. If convicted of the offence under the Income Tax Act, a fine not exceeding \$1000 may be imposed and in default of payment, imprisonment for a term not exceeding 6 months. If convicted of the offence under the Goods and Services Tax Act, a fine not exceeding \$5000 may be imposed or imprisonment for a term not exceeding 6 months or both.

6 Storage Media & File Format for Tax Audit Purposes

When imaged documents are required by the Comptroller's representative in the course of a tax audit, the taxpayer should have facilities to output the image in both hard or soft copies. Soft copies of the documents should be made available on any of the following media options and graphic file formats:

- (a) Saved in CD-Rom, DVD-Rom, 1.44MB floppy diskettes, Iomega ZIP diskettes or IDE hard disks; and
- (b) Graphic files should be recorded in GIF, TIF or JPG formats.

The above media and data formats are specified because they are common media and data formats which IRAS has the facilities to handle. IRAS will be prepared to consider other media and data formats on a case by case basis, provided IRAS has the facilities to handle such media or data formats.