Privacy Commissioner
Te Mana Matapono Matatapu

Information Matching Compliance Auditing Information Pack

ISBN 0-478-11731-0
4th edition 2010

1st edition June 2007
2nd edition February 2008
3rd edition March 2009

Further copies are available from
the Office of the Privacy Commissioner
website: www.privacy.org.nz

Privacy Commissioner
PO Box 10094
The Terrace
Wellington 6143
New Zealand

Telephone 04 474 7590
Facsimile 04 474 7595
Email enquiries@privacy.org.nz

CONTENTS

Introduction

Guidelines

Audit Templates

Reference Materials

Introduction

> *Computer matching is a powerful dataveillance technique, capable of offering benefits in terms of the efficiency and effectiveness of government business greater than its financial costs. … Unless a suitable balance is found, and controls imposed which are perceived by the public to be appropriate and fair, its use will result in inappropriate decision-making and harm to people's lives. In a tightly controlled society this is inequitable. In a looser, more democratic society, it risks a backlash by the public against the organisations that perform it, and perhaps the technology that supports it.*
> - Roger Clarke, *A Normative Regulatory Framework for Computer Matching*, 1995

The Privacy Act (the Act) regulates the practice of information matching in the public sector through the controls in Part 10 of the Act and the rules in Schedule 4. These controls are designed to minimise privacy risks and help maintain public confidence in the fair handling of data.

The Act places a special responsibility upon the Privacy Commissioner to oversee authorised information matching programmes. One way in which the Commissioner performs that oversight is by requiring agencies to audit and report on their activities. The audit approach has been developed to enhance regulatory oversight and provide insights into areas where traditional statistical reporting have been less useful.

The audit approach assesses compliance with the information matching controls in two parts. The first, called the **documentation audit**, looks at agency documentation, policies, forms, and guidelines. The second, called the **process audit**, focuses upon the agency management and staff involved in operating the programme.

Feedback from agencies using the audit approach continues to be positive with useful suggestions helping us to update audit materials. We welcome feedback that enables the audit approach to be further enhanced.

Policy and Technology Team
Office of the Privacy Commissioner

Guidelines

Audit Objective

- To obtain evidence to enable the Commissioner to be satisfied that each programme operates in compliance with the information matching controls in the Act.

Who Should Perform the Audit?

- Auditors should be independent of the function being audited. Ideally the auditor will have an auditing qualification and/or proven experience in auditing or risk assurance. Consideration should be given to having a multi-person audit team to assist with interviewing and note taking.

Undertaking the audit

- Where multiple audits for a programme fall due in one year (such as a s.104 audit and an online transfer audit), please discuss scheduling with us as there may be scope for performing these audits together.

- It is best to use the checklists in Appendices A and B, but it may be necessary or useful to adjust or supplement the checklist in some cases.

- Auditors should collect enough information in order to draw sound conclusions on compliance.

- Auditors may find that while there may be no specific controls designed to achieve Privacy Act compliance, there may be other controls that achieve the desired effect. Auditors need to be alert to these controls as they may not be easily identified.

- Auditors may not be able to audit to the level required to *guarantee* that an agency is compliant, as a review of extensive evidence may be uneconomic. It may be necessary to rely on certain assurances by a suitably senior person in the agency.

- Samples of information collected should be representative of the year under review (e.g. more than one match run).

- Interviews should involve a selection of staff rather than a single office expert. Oversight of a sample of work being undertaken is useful to confirm that work practices mirror the responses provided to the audit questions.

- Some questions can only be answered by staff from the agency that supplies the information (source agency); some by the agency that uses the results generated by the programme (user agency) and a few require an answer from both. Usually either the source or user agency carry out the process of comparison. However, if this function were outsourced to a service provider, questions would need to be directed there.

- Large scale matching operations may involve separation of duties. For instance, there may be different staff involved in assessing raw results, initiating adverse action, and handling challenges. Auditors must ensure they are asking the right group of staff the most appropriate question.

- Documentary evidence is usually more reliable than oral evidence.

- Where documentation suggests a non-compliance issue, it is wise to see what happens in practice before coming to a formal conclusion.

Documenting Audit Findings

- Audit findings emerge through a process of comparing ‘what should be’ with ‘what is’. Where there is a difference, the auditor should complete an assessment of the consequences and their severity.

- Where criteria are not being met, a negative conclusion is required. The auditor must consider the significance of the weakness and make recommendations for resolution. If the criteria are met the auditor can then report a positive conclusion.

- Where auditors feel they have been unable to obtain adequate evidence to base any conclusions, this should be reflected in the statements of assurance.

Preparing the Draft Report

- The report should be unbiased in tone. It should note good performance and credit management for actions taken to correct deficiencies.

- Agencies must be given the chance to respond to findings. This is to:
    - reduce the risk of conclusions that may be inappropriate;
    - ensure there are no misunderstandings / misinterpretations of fact; and
    - ensure that the auditor is aware of all relevant information.

- The auditor should report on each part of the audit, but only significant adverse findings require recommendations.

- Action points should be agreed before final sign off.

- The template in Appendix C outlines the minimum reporting requirements and should normally be used. However, variations for good reason may well be fine. Please contact us in advance if you are planning to significantly depart from the template as this will make things clearer for us and save time later.

Appendix A: Information Matching Documentation Audit Checklist

Organisation		**Programme Name**			
Aspect	**Documentation Review**	**Auditor**		**Interviewees**	

Purpose of this checklist: To assess to what extent the documentation reflects the requirements of the Information Matching provisions in the Privacy Act 1993.

When to use this document: The Documentation Audit is step 1 in the audit process. It should be completed in advance of the Process Audit (step 2).

How to use this document:

- View departmental documents that demonstrate compliance with items listed under **Information Matching Requirement** in the left column.
- Record the document name and date (where applicable) under **document reference(s)**.
- Record any observations you have under **comments.**
- Mark your **Result** decision as follows:
  - **AA** = Issue addressed adequately (no apparent issues identified in complying with the information matching requirement)
  - **NAA** = Issue not addressed adequately (aspects of the information matching requirement not fully met)
  - **NR** = No reference found to issue in documentation (lack of documentation to deal with specific information matching requirement)

Information Matching Requirement	Document reference(s)	Comments	Result
1 Information Matching Agreement (IMA) (Privacy Act 1993 - section 99)			
a) A signed IMA is held by each agency. Record who has signed it. Ensure any amendments to the IMA have also been signed.			
b) If a new IMA or an amendment to an existing IMA were entered into during the year, was a copy forwarded to the Privacy Commissioner?			

Appendix A: Information Matching Documentation Audit Checklist			
Information Matching Requirement	**Document reference(s)**	**Comments**	**Result**
1 Information Matching Agreement (IMA) (Privacy Act 1993 - section 99) continued			
c) Confirm that the IMA incorporates provisions that reflect the Information Matching Rules or has equivalent controls documented. (see Appendix E – Schedule 4: Information Matching Rules) Information matching rules: 1. Notice to individuals affected 2. Use of unique identifiers 3. Online transfers 4. Technical standards 5. Safeguards for individuals affected by results of programmes 6. Destruction of information 7. No new databank 8. Time limits			

Appendix A: Information Matching Documentation Audit Checklist			
Information Matching Requirement	**Document reference(s)**	**Comments**	**Result**
2 Technical Standards Report (Privacy Act 1993 – Schedule 4 Information Matching Rule 4)			
a) A copy of the Technical Standards Report (TSR) (and any variations) is held by all agencies involved in the programme			
b) If a new TSR or a variation to a TSR was completed during the year, was a copy provided to the Privacy Commissioner?			
c) The TSR document must be maintained by the agency primarily responsible for the operation of the programme. (See Appendix E - Schedule 4, Rule 4 Technical Standards). Details about the following must be included in the TSR: 1. The integrity of the information to be matched (including key terms and definitions, relevance, timeliness, and completeness) 2. The matching techniques with particular reference to: ▪ The matching algorithm ▪ Any use of unique identifiers ▪ The nature of matters being sought ▪ The relevant information definitions ▪ The procedure for recognising matches 3. The controls to ensure continued integrity of the programme, including procedures to confirm validity of matching results. 4. The security features, including details about how information is transferred between agencies.			

Appendix A: Information Matching Documentation Audit Checklist			
Information Matching Requirement	**Document reference(s)**	**Comments**	**Result**
3 Notices of Adverse Action (Privacy Act 1993 - section 103)			
The agency involved in taking adverse action has in place a written section 103 type notice which details: ▪ Particulars of the discrepancy and the action it proposes to take ▪ States that the individual has 5 working days from the receipt of the notice to challenge the information Review the template version of the s.103 notice if applicable for compliance with the notice requirements. View a sample of s.103 notices sent to confirm compliance with the notice requirements.			
4 Notice to Individuals Affected (Privacy Act 1993 - Information Matching Rule 1)			
Note the ways the Agencies comply with Information matching Rule 1 regarding public notification of the programme, eg website, pamphlets, notices on application forms, etc.			
5 Online Transfers (Privacy Act 1993 - Information Matching Rule 3)			
If the programme has utilised online computer connections during the year confirm that there is a current Online Transfer Approval from the Privacy Commissioner.			

Appendix B: Information Matching Process Audit Checklist

Organisation		**Programme Name**			
Aspect	**Process Review**	**Auditor**		**(Names of interviewees)**	

Purpose of this Checklist: To assess the extent that operational practices support and reflect the requirements of the Privacy Act 1993, Part 10 and Schedule 4.

When to use this document: Following completion of the Documentation Audit. Once the Documentation Audit and Process Audit are complete, the final audit report can be completed.

How to use this document: This document is divided into 2 sections, one for management responses and one for staff responses. Questions are prefixed with either M for management or S for staff along with a number.

- Record responses and note any supporting documents provided.
- Comment on the responses / documents provided under "findings and observations".
- Mark the result in the right hand column. Your findings and observations should support your Result decision
- COM = Complies (no issues identified)
- MAJ = Major Non-compliance (ongoing and systemic breach that may result in serious consequences for individuals affected)
- MIN = Minor Non-compliance (one off breaches usually as a result of human error, with minor impact on individuals affected)

All bracketed legal references refer to the Privacy Act 1993.

Section 1: Management responses for questions prefixed M1 – M6

Question/Check	Responses and Supporting Documents Examined	Findings and Observations	Result
M1 How does the agency ensure that new / existing staff / managers maintain an awareness of Privacy Act requirements in their work? Describe the nature of any Privacy Act training.			

Appendix B: Information Matching Process Audit Checklist			
Question/Check	**Responses and Supporting Documents Examined**	**Findings and Observations**	**Result**
M2 What controls are in place to prevent unauthorised access to personal information supplied for, or produced by the programme? For example: Limited access rights to physical areas. Restricted access to data via application controls. Routine access audits / monitoring. [Principle 5]			
M3 How do you know if the matching programme is being operated in accordance with the technical standards report? Are there any regular reviews of operations? [Schedule 4, Rule 4]			
M4 Identify what uses are made of the information provided from the programme. [Schedule 3 – each information matching provision limits the allowable uses of information disclosed in an authorised matching programme].			
M5 Describe the process(es) in place to ensure that information supplied for, or produced by, the programme is deleted after it is no longer needed? [s. 101; Schedule 4, Rule 6]			

Appendix B: Information Matching Process Audit Checklist			
Question/Check	**Responses and Supporting Documents Examined**	**Findings and Observations**	**Result**
M6 Describe the processes in place to generate statistical programme reporting (if applicable). What quality control features exist to ensure that programme reporting is accurate and timely? [s. 104 – reporting requirements]			

Appendix B: Information Matching Process Audit Checklist

Section 2: Staff responses for questions prefixed S1 – S11

Question/Check	Responses and Supporting Documents Examined	Findings and Observations	Result
S1 Describe your training in the Privacy Act 1993.			
S2 What Privacy Act rules are you aware of when doing your work?			
S3 Do you have easy access to user documentation? Examples might include: Procedure manuals, Online help files / systems			
S4 Is documentation easy to follow and cover all aspects of operations? Describe any areas which you believe need improvement.			
S5 When no match or a partial (inexact) match occurs, how do you verify an individual's identity? Are there set processes to follow? [Schedule 4, Rules 4 and 5]			

Appendix B: Information Matching Process Audit Checklist			
Question/Check	**Responses and Supporting Documents Examined**	**Findings and Observations**	**Result**
S6 Do you contact the other agency involved in the programme when verifying the results of a match? If so, what is the process? [Schedule 4, Rule 5]			
S7 When you match an individual and decide to take some action against them, how do you notify them? What is the procedure? [s.103]			
S8 Describe the process for reporting and resolving mistakes made during the operation of the matching process. Do mistakes occur often? [s. 104]			
S9 Generally, how many days is it before you decide to take action against an individual as a result of a data match? [s. 101]			

Appendix B: Information Matching Process Audit Checklist			
Question/Check	**Responses and Supporting Documents Examined**	**Findings and Observations**	**Result**
S10 When your agency receives information from another agency for the programme, what happens to the information once you have finished processing? Describe the process(es) in place to ensure that matching information is deleted after it is no longer needed. [s.101; Schedule 4, Rule 6]			
S11 Do you keep the information that you received from the other agency for the programme for another purpose? [Legislative provisions listed in Schedule 3 define the allowable purpose(s) of a matching programme. Matching must also be done in accordance with the Technical Standards Report (Schedule 4, Rule 4)]			

Appendix B: Information Matching Process Audit Checklist
Other questions and comments arising from management or staff responses / aspects of the programme not already covered

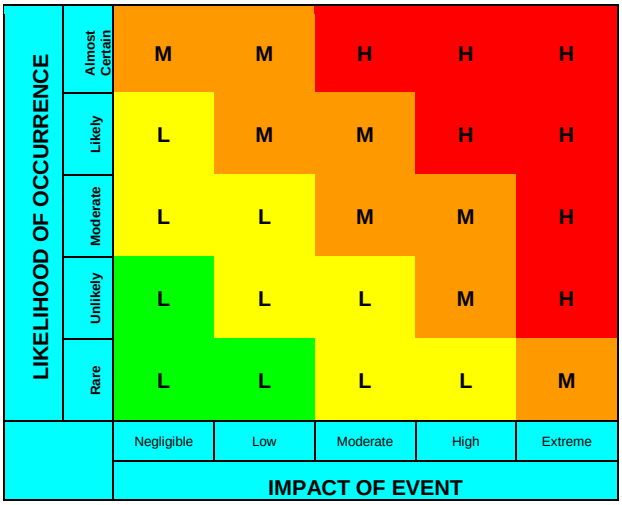
Appendix C:
Information Matching Compliance Audit Report Template

Executive Summary / Audit Objective

This section should contain a short overview of the programme and details of the request by the Privacy Commissioner to provide an audit report under s.104 of the Privacy Act. It should also explain that the Privacy Commissioner requires the audit to assess whether the programme is being operated compliantly with ss.99 to 103 of the Privacy Act and the Information Matching Rules.

Priority of Issues Reported / Risk Rating

This section should explain how the priority of each issue in the report has been rated based on an assessment of the impact or consequence of the risk and the likelihood of its occurrence. The risk matrix below (based upon an adaptation of AS/NZS 4360 2006 Risk Management) can be used to calculate High (H), Moderate (M) or Low (L) rating outcomes.



Audit Scope

This section should explain the scope of the audit. For example, that it is limited to the questions/checks contained in the Information Matching Documentation Audit Checklist and the Information Matching Process Audit Checklist. It should also note whether the audit assesses any of the wider information handling practices of the department that may relate to the information matching programme.

Audit Approach

This section should provide an outline of the steps taken to complete the audit. Include details about the documents sighted and which agency staff were interviewed.

Conclusion

Include matters of significance here. Related observations can be aggregated and addressed with higher level recommendations, eg to improve controls.

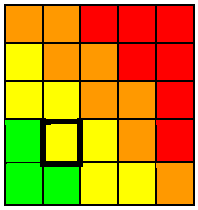
Table summary

Component	Rating
Overall rating:	
Information Matching Agreement (Documentation Audit 1a, b, c)	
Technical Standards Report (Documentation Audit 2a, b, c; 3; 5)	
Matching process and confirmation procedures (Process Audit M4, S5, S6, S8, S9)	
Notices to individuals (Documentation Audit 4, Process Audit S7)	
Storage, security and destruction of information Process Audit M2, M3, M5, S10, S11	
Staff training practices Process Audit M1, S1, S2	
User documentation Process Audit M1, M6, S3, S4	

Rating Key	Description
Green	Effective controls / activities in place, no issues identified
Yellow	Effective controls / activities, minor issues identified or some compensating controls exist
Orange	Partially effective controls / activities in place, moderate or low risk issues identified
Red	Ineffective controls / activities in place

Detailed discussion of each issue identified

Detail any issue and assign a priority / risk weighting. Mark the rating on the matrix table.



Recommendations

Detail action points to correct identified issue.

Management response

Management's response to the recommendations raised in the audit report and the actions to be undertaken to address recommendations.

Responsibility

Identify the person responsible for undertaking the agreed actions.

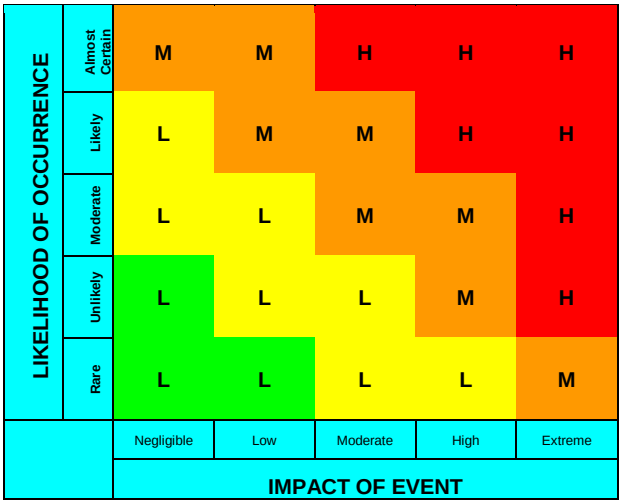
Completion date

Date for completing agreed actions.

Agency and Auditor sign off

To be completed by an appropriate management level for both agency and auditor.

Appendix D:
Guidance note: Using the risk assessment matrix table



The risk assessment matrix table assists an auditor to assign a risk rating. An overall risk rating is based on the combination of the **impact** or consequence of the risk and the **likelihood** of its occurrence. For instance, for an issue which has a ***moderate*** impact and is ***likely*** to occur, the outcome is a ***moderate*** risk rating.

Determining the risk impact rating

Determining a single risk impact value may prove to be difficult as there is likely to be a range of consequences that result from any given event.

For instance, consider the scenario where a staff member in agency A has legitimate access to records in agency B to enable the processing of a client application. If there are weak audit/security management controls in place there may be a risk of inappropriate browsing or use of that information. The impact of any event will depend on the intent of the staff member. The impact may be **low** in the case of minor browsing to **high** where malice or criminal intent may result in significant harm to an individual. The impact assessment will need to consider aggravating factors such as the amount of data and its sensitivity.

Ongoing and systematic breaches will result in a higher impact risk assessment than one-off events that have occurred as a result of human error.

A risk averse approach to risk impact assessment is to identify the worst-case scenario and develop a response that mitigates that level or impact. That response will probably also deal with any lower level impacts.

Determining the risk likelihood rating

After identifying the level of impact, the next step is to consider the likelihood that the risk event will occur. The table below provides guidance on how to determine the likelihood rating.

Risk Likelihood Ratings	
Likelihood	**Description**
Almost Never/Rare [**1**]	The risk event may occur only in exceptional circumstances, eg up to 4% chance of occurring in the next 12 months (or once in 25 years).
Unlikely [**2**]	The risk event could occur at some time, eg 10% chance of occurring in the next 12 months or 1 out of every 10 years.
Moderate/ Possible [**3**]	The risk event could occur at some time, eg 25% chance of occurring in the next 12 months or 5 out of every 20 years.
Likely [**4**]	The risk event will probably occur in most circumstances, eg 55% chance of occurring in the next 12 months or 11 out of every 20 years.
Almost Certain [**5**]	The risk event is expected to occur in most circumstances, eg 90% chance of occurring in the next 12 months or 18 out of every 20 years.

Appendix E: Extracts from the Privacy Act 1993

Note: These extracts are provided for convenience, but it is recommended that auditors obtain a complete and up to date copy of the Act (particularly Part 10 and Schedule 4) for themselves.

Selected Definitions

Adverse action – ref. Privacy Act 1993, Part 10, section 97

adverse action means any action that may adversely affect the rights, benefits, privileges, obligations, or interests of any specific individual; and, without limiting the generality of the foregoing, includes any decision--

(a) to cancel or suspend any monetary payment;

(b) to refuse an application for a monetary payment;

(c) to alter the rate or amount of a monetary payment;

(d) to recover an overpayment of a monetary payment;

(e) to make an assessment of the amount of any tax, levy, or other charge, or of any contribution, that is payable by any individual, or to alter any such assessment;

(f) to investigate the possible commission of an offence; and

(g) to deport the individual from New Zealand, or to revoke the individual's permit or visa entitling the individual to enter or remain in New Zealand or to make or execute a removal order.

Discrepancy – ref. Privacy Act 1993, Part 10, section 97

discrepancy, in relation to an authorised information matching programme, means a result of that programme that warrants the taking of further action by any agency for the purpose of giving effect to the objective of the programme

Information Privacy Principle 5 – ref. Privacy Act 1993, section 6

Storage and security of personal information

An agency that holds personal information shall ensure—

(a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against—

(i) loss; and

(ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and

(iii) other misuse; and

(b) that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the

power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

s.99 Information matching agreements

(1) No personal information held by any specified agency shall be disclosed, pursuant to an information matching provision, to any other specified agency for the purposes of an authorised information matching programme except pursuant to a written agreement between those agencies.

(2) Every such agreement shall incorporate provisions that reflect the information matching rules, or provisions that are no less onerous than those rules, and the agencies that are parties to the agreement shall comply with those provisions.

(3) Any such agreement may provide that the agencies involved in the information matching programme may charge each other fees for the services provided for the purposes of the programme.

(4) The parties to an agreement entered into pursuant to this section shall ensure that a copy of the agreement, and of any amendments subsequently made to such an agreement, are forwarded to the Commissioner forthwith.

s.101 Further provisions relating to results of information matching programme

(1) Notwithstanding anything in section 100, where—

(a) a specified agency derives or receives information produced by an authorised information matching programme; and

(b) as a result of deriving or receiving that information, the agency becomes aware of a discrepancy,—

that agency shall destroy that information not later than the expiration of the period of 60 working days after the agency becomes aware of that discrepancy unless, before the expiration of that period, the agency has considered that information and made a decision to take adverse action against any individual on the basis of that discrepancy.

(2) Any adverse action commenced by a specified agency in accordance with subsection (1) shall be commenced not later than 12 months from the date on which the information was derived or received by the agency.

(3) Where a specified agency decides not to take adverse action against any individual on the basis of information produced by an authorised information matching programme, the agency shall as soon as practicable destroy the information.

(4) When information produced by an authorised information matching programme is no longer needed by a specified agency for the purposes of taking any adverse action against any individual, the agency shall as soon as practicable destroy the information.

(5) Nothing in this section applies in relation to the Inland Revenue Department.

s.103 Notice of adverse action proposed

(1) Subject to subsections (1A) to (2A), a specified agency shall not take adverse action against any individual on the basis (whether wholly or in part) of a discrepancy produced by an authorised information matching programme—

(a) unless that agency has given that individual written notice—

(i) specifying particulars of the discrepancy and of the adverse action that it proposes to take; and

(ii) stating that the individual has 5 working days from the receipt of the notice in which to show cause why the action should not be taken; and

(b) until the expiration of those 5 working days.

(1A) Nothing in subsection (1) shall prevent the department for the time being responsible for the administration of the Social Security Act 1964 from immediately suspending a sickness, training, unemployment, independent youth, or emergency benefit, or a job search allowance, paid to an individual where the discrepancy arises in respect of departure information supplied to that Department pursuant to section 280 of the Customs and Excise Act 1996, and where, before or immediately after the decision to suspend, the Department gives the individual written notice—

(a) specifying particulars of the discrepancy and the suspension of benefit, and any other adverse action the Department proposes to take; and

(b) stating that the individual has 5 working days from the receipt of the notice to show cause why the benefit ought not to have been suspended or why the adverse action should not be taken, or both—

and the adverse action shall not be taken until the expiration of those 5 working days.

(1B) Nothing in subsection (1) prevents the Commissioner of Inland Revenue from immediately suspending payment to an individual of all or part of an interim instalment of a credit of tax under subpart KD of the Income Tax Act 2004 when a discrepancy is identified in information supplied to the Commissioner under section 85G of the Tax Administration Act 1994 if, before or immediately after the decision to suspend, the Commissioner gives a written notice to the individual that—

(a) provides details of the discrepancy and the suspension of payment of the credit of tax and any other adverse action which the Commissioner proposes to take; and

(b) states that the individual has 5 working days from the receipt of the notice to show cause why payment of the credit of tax ought not to have been suspended or why the adverse action should not be taken, or both—

and the other adverse action must not be taken until expiration of those 5 working days.

(2) Nothing in subsection (1) or subsection (1A) or subsection (1B) prevents an agency from taking adverse action against an individual if compliance with the requirements of that subsection would prejudice any investigation into the commission of an offence or the possible commission of an offence.

(2A) Nothing in subsection (1) prevents any sworn member of the police or any bailiff from immediately executing a warrant to arrest an individual in respect of the non-payment of the whole or any part of a fine if the discrepancy arises in respect of arrival and departure information supplied under section 280D of the Customs and Excise Act 1996 and if, before executing the warrant, the individual concerned is—

(a) informed of the intention to execute the warrant; and

(b) given an opportunity to confirm—

(i) whether or not he or she is the individual named in the warrant; and

(ii) that neither of the following circumstances applies:

(A) the fine has been paid; or

(B) an arrangement to pay the fine over time has been entered into.

(3) Every notice required to be given to any individual under subsection (1) or subsection (1A) or subsection (1B) may be given by delivering it to that individual, and may be delivered—

(a) personally; or

(b) by leaving it at that individual's usual or last known place of residence or business or at the address specified by that individual in any application or other document received from that individual; or

(c) by posting it in a letter addressed to that individual at that place of residence or business or at that address.

(4) If any such notice is sent to any individual by post, then in the absence of proof to the contrary, the notice shall be deemed to have been delivered to that individual on the fourth day after the day on which it was posted, and in proving the delivery it shall be sufficient to prove that the letter was properly addressed and posted.

(5) In this section,—

bailiff means a bailiff of the District Court or of the High Court.

fine means—

(a) a fine within the meaning of section 79 of the Summary Proceedings Act 1957 or an amount of reparation:

(b) a fine or other sum of money to which any of sections 19 to 19E of the Crimes Act 1961 applies:

(c) a fine to which any of sections 43 to 46 of the Misuse of Drugs Amendment Act 1978 applies.

reparation means—

(a) any amount that is required to be paid under a sentence of reparation; or

(b) any amount that is required to be paid under any order of reparation as defined in section 145D of the Sentencing Act 2002.

Schedule 4: Information matching rules

1 Notice to individuals affected

(1) Agencies involved in an authorised information matching programme shall take all reasonable steps (which may consist of or include public notification) to ensure that the individuals who will be affected by the programme are notified of the programme.

(2) Nothing in subclause (1) requires an agency to notify any individual about an authorised information matching programme if to do so would be likely to frustrate the objective of the programme.

2 Use of unique identifiers

Except as provided in any other enactment, unique identifiers shall not be used as part of any authorised information matching programme unless their use is essential to the success of the programme.

3 On-line transfers

(1) Except with the approval of the Commissioner, information transferred between agencies for the purposes of an authorised information matching programme shall not be transferred by means of on-line computer connections.

(2) Any approval given under subclause (1) may be given either unconditionally or subject to such conditions as the Commissioner thinks fit.

(3) Any approval given under subclause (1) may at any time be withdrawn by the Commissioner; and any condition subject to which any such approval is given may from time to time be revoked, varied, or added to by the Commissioner.

4 Technical standards

(1) The agency primarily responsible for the operation of an authorised information matching programme shall establish and maintain detailed technical standards to govern the operation of the programme.

(2) The technical standards established by an agency in accordance with subclause (1) shall deal with the following matters:

(a) the integrity of the information to be matched, with particular reference to—

(i) key terms and their definition; and

(ii) relevance, timeliness, and completeness:

(b) the matching techniques to be used in the programme, with particular reference to—

(i) the matching algorithm:

(ii) any use of unique identifiers:

(iii) the nature of the matters being sought to be identified by the matching process:

(iv) the relevant information definitions:

(v) the procedure for recognising matches.

(c) the controls being used to ensure the continued integrity of the programme, including the procedures that have been established to confirm the validity of matching results:

(d) the security features included within the programme to minimise and audit access to personal information, including the means by which the information is to be transferred between agencies.

(3) The technical standards established in accordance with subclause (1) shall be incorporated in a written document (in this clause called a Technical Standards Report), and copies of the Technical Standards Report shall be held by all agencies that are involved in the authorised information matching programme.

(4) Variations may be made to a Technical Standards Report by way of a Variation Report appended to the original Report.

(5) The agency that prepares a Technical Standards Report shall forward a copy of that report, and of every Variation Report appended to that report, to the Commissioner.

(6) The Commissioner may from time to time direct that a Technical Standards Report be varied, and every such direction shall be complied with by the agency that prepared the Report.

(7) Every agency involved in an authorised information matching programme shall comply with the requirements of the associated Technical Standards Report (including any variations made to the report).

5 Safeguards for individuals affected by results of programmes

(1) The agencies involved in an authorised information matching programme shall establish reasonable procedures for confirming the validity of discrepancies before any agency seeks to rely on them as a basis for action in respect of an individual.

(2) Subclause (1) shall not apply if the agencies concerned consider that there are reasonable grounds to believe that the results are not likely to be in error, and in forming such a view regard shall be had to the consistency in content and context of the information being matched.

(3) Where such confirmation procedures do not take the form of checking the results against the source information, but instead involve direct communication with the individual affected, the agency that seeks to rely on the discrepancy as a basis for action in respect of an individual shall notify the individual affected that no check has been made against the information which formed the basis for the information supplied for the programme.

(4) Every notification in accordance with subclause (3) shall include an explanation of the procedures that are involved in the examination of a discrepancy revealed by the programme.

6 Destruction of information

(1) Personal information that is disclosed, pursuant to an information matching provision, to an agency for use in an authorised information matching programme and that does not reveal a discrepancy shall be destroyed as soon as practicable by that agency.

(2) Where—

(a) personal information is disclosed, pursuant to an information matching provision, to an agency for use in an authorised information matching programme; and

(b) that information reveals a discrepancy,—

that information shall be destroyed by that agency as soon as practicable after that information is no longer needed by that agency for the purposes of taking any adverse action against any individual.

(3) Nothing in this clause applies in relation to the Inland Revenue Department.

7 No new databank

(1) Subject to subclauses (2) and (3), the agencies involved in an authorised information matching programme shall not permit the information used in the programme to be linked or merged in such a way that a new separate permanent register or databank of information is created about all or any of the individuals whose information has been subject to the programme.

(2) Subclause (1) does not prevent an agency from maintaining a register of individuals in respect of whom further inquiries are warranted following a discrepancy revealed by the programme, but information relating to an individual may be maintained on such a register only for so long as is necessary to enable those inquiries to be carried out, and in no case longer than is necessary to enable any adverse action to be taken against an individual.

(3) Subclause (1) does not prevent an agency from maintaining a register for the purpose of excluding individuals from being selected for investigation, but such register shall contain the minimum amount of information necessary for that purpose.

8 Time Limits

1) Where an authorised information matching programme is to continue for any period longer than 1 year, or for an indefinite period, the agencies involved in the programme shall establish limits on the number of times that matching is carried out pursuant to the programme in each year of its operation.

(2) The limits established in accordance with subclause (1) shall be stated in writing in an annex to the Technical Standards Report prepared in respect of the programme pursuant to clause 4 of this Schedule.

(3) The limits established in accordance with subclause (1) may be varied from time to time by the agencies involved in the programme.