GOOD PRACTICE GUIDE FOR IDENTITY FRAUD CONTROL

Identity Assurance Framework

INTERNAL AFFAIRS

Te Tari Taiwhenua

CONTENTS

FOREWORD:
THE CASE FOR IMPROVING YOUR INTERNAL CONTROLS TO COMBAT IDENTITY FRAUD

Identity fraud is a serious issue for organisations throughout New Zealand. Whether perpetrated by employees, contractors, customers or suppliers, it has significant and often long-term economic and social costs – not only for the organisations themselves, but for those affected through its flow-on effects. Identity fraud affects the whole economy.

The Department of Internal Affairs has conservatively estimated the financial costs of identity fraud to the New Zealand economy at $136 million to $204 million per annum, and the costs to public sector agencies at $22 million to $33 million.

HOW DOES FRAUD HAPPEN?

In 2010 KPMG conducted a 'fraud and misconduct' survey of a representative sample of large organisations in the public and private sectors in Australia and New Zealand.[1]

A key conclusion was that the most important factors contributing to the largest fraud incidents were 'override of internal controls' and 'poor internal controls'.

Internal controls are also the biggest fraud-detection tool in New Zealand, with nearly half of all cases (49%) detected this way.

WHY DOES FRAUD HAPPEN?

Fraud generally happens because of:

- motivation, such as a need for money or to access a service and/or cause disruption;
- opportunity, such as weakness in an organisation's internal controls; and
- personal characteristics, such as a willingness to commit fraud.[2]

[1] Released in 2010, the survey is conducted biennially. **www.kpmg.com/NZ/en/IssuesAndInsights/ArticlesPublications/Pages/Fraud-Survey-2010.aspx**

[2] Adapted from Modified Understanding Internal Controls: A Reference Guide for Managing University Business Practices. **www.ucop.edu/ctlacct/under-ic.pdf**

WHAT CAN WE DO TO COMBAT FRAUD?

To date, organisational efforts to combat fraud have tended to limit their scope to:

- influencing the motivation to commit internal fraud, such as through ensuring adequate pay and conditions for staff; and

- personal characteristics, such as through promoting ethical standards and undertaking careful pre-employment screening and recruitment.

However, the risks and incidences of fraud can also be significantly reduced through developing (and continually improving) effective internal control systems. That is what the *Guide* is about.

INTRODUCING THE GUIDE

The *Good Practice Guide for Identity Fraud Control* is designed to help your organisation minimise the risks of identity fraud through effective and sustained internal controls.

It has been developed by the Department of Internal Affairs, which works closely with the wider identity management community to ensure that:

- identity information is well governed, so that organisations and individuals in New Zealand can be reassured that their identity information is protected by processes, systems and people with high levels of integrity;

- people can access services that have an identity component easily, efficiently and cost effectively; and

- identity information is kept secure and is effectively managed, protecting people from fraud and meeting their reasonable expectations for privacy and civil liberties.[3]

COMPLEMENTARY, CROSS-GOVERNMENT INITIATIVES

The *Guide* is connected to and complements a wider programme of government initiatives that support good identity information management practice. They include:

- the Identity Common Capability Programme, which includes the development of a range of shared services such as the igovt services and the Data Validation Service to support better, smarter identity information management for less;

- the *Evidence of Identity Standard (EOI Standard)*;[4] and

- the Department of Labour's Identity Management Programme, which includes the development of modern identity assurance systems and services for non-New Zealand citizens.

The *Guide* is an important tool for detecting, preventing and responding to identity fraud. Please use it – and let us know what you think. It is a 'living document', and we need your feedback to ensure it continues to be relevant and useful for organisations throughout the country.

Andrea Gray
Manager, Integrity and Identity Programmes
Department of Internal Affairs

....
[3]Department of Internal Affairs' *Statement of Intent 2010-2013.*
www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Corporate-Publications-Statement-of-Intent-2010-13?OpenDocument

[4]**www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Evidence-of-Identity-Standard-Index or https://psi.govt.nz/evidence/default.aspx**

1.0
INTRODUCTION

This *Good Practice Guide for Identity Fraud Control* (the *Guide*) has been developed by the Department of Internal Affairs to help organisations throughout New Zealand minimise the risks of identity fraud. It is part of work to achieve the goals of Government's *Identity Assurance Framework*.[5]

The *Guide* is particularly suitable for organisations that deliver services with identity-related risks – both from outside (involving customers and suppliers) and from within (involving staff and third-party contractors). Within organisations, the *Guide* will be of particular interest to those responsible for fraud control, such as:

• senior management personnel;

• policy and business advisors/analysts;

• investigators;

• risk management and assurance advisors/ analysts;

• communications staff (for raising staff and public awareness); and

• legal advisors.

The *Guide* is not mandatory; however, the Department of Internal Affairs recommends it is considered by organisations with identity-related risk. Use of the *Guide* should complement any fraud-control systems you already operate.

1.1 INTEGRATED MANAGEMENT FRAMEWORK

Identity fraud is often a precursor for other fraudulent activities, such as falsely claiming benefit payments, falsely applying for financial credit and committing terrorist acts. To minimise the risks of it happening to your organisation (as well as the downstream impacts for your and other organisations), it is vital that you establish your own internal controls for identity fraud prevention, detection and response.

By 'controls' we mean policies, procedures, techniques and mechanisms that aim to minimise process failures and ensure action is taken to address risks. Ideally, these controls help to mitigate the risks of identity fraud, as well as help you to deliver high standards of service to your customers.

The *Guide* provides an integrated management framework for identity fraud control, based on:

• clear governance arrangements;

• systems and structures designed to prevent, detect and respond to identity fraud; and

• a method for monitoring your identity fraud results against specified performance measures and, where required, adapting your fraud controls accordingly.

---

[5] *The Identity Assurance Framework* is moving government to a future state through seven transformation categories. These seven categories provide assurance to the public that identity is being managed appropriately and effectively within government, while maintaining privacy. **www.dia.govt.nz/ diawebsite.nsf/wpg_URL/Resource-material-Publications-Identity-Assurance-Framework?OpenDocument**

How the framework works
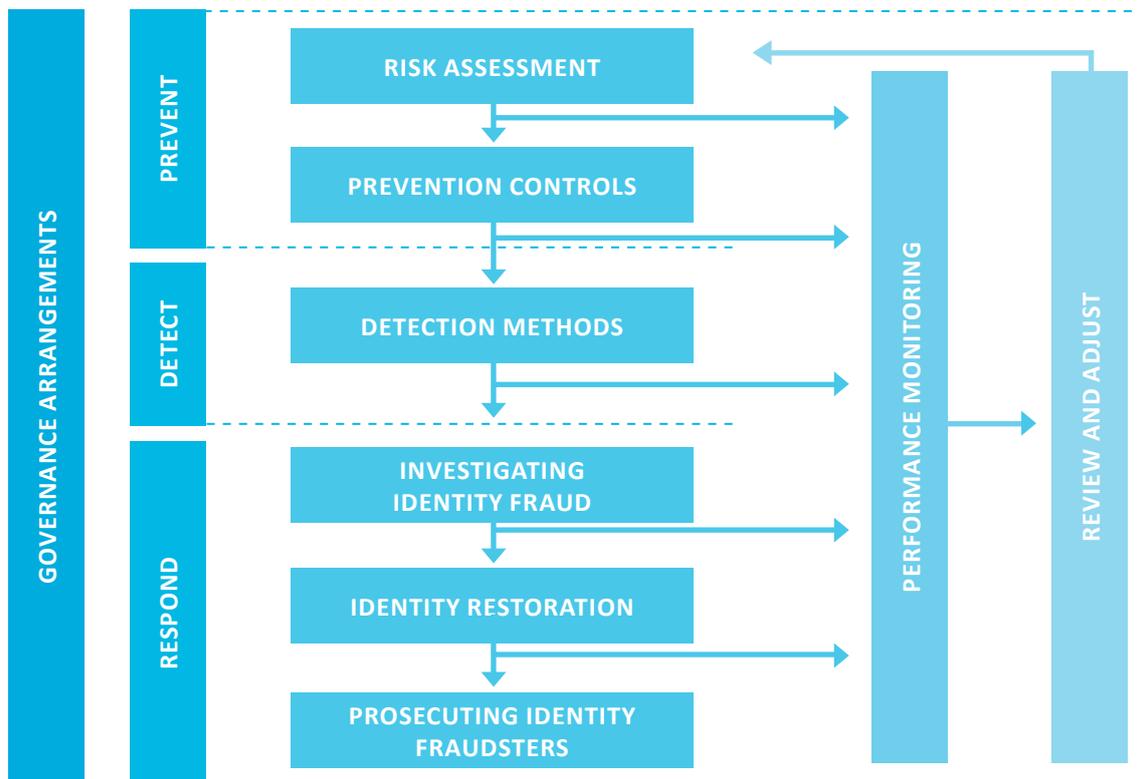
The *Guide* discusses each element of the framework in detail, outlining your organisational responsibilities and providing short checklists to help you deliver on them. It also includes an explanation of the terminology used, which you will find on page 37.

Note the *Guide* is a living document that will be updated periodically to reflect organisational demands and international and domestic developments and trends.

A note about external guidance

The *Guide* includes a number of references to other external resources and more detailed guidance on particular aspects of identity fraud

control. The external guidance (italicised in the text and detailed in footnotes) is provided for background information only and is not endorsed by the Department of Internal Affairs. You can read a full reference list at the end of the *Guide* on page 39, but owing to the changing nature of the internet, links to websites may not operate. Please report any access difficulties to ICCP@dia.govt.nz.

For more information about the I*dentity Assurance Framework* and this *Guide*, please contact the Department of Internal Affairs at ICCP@dia.govt.nz.

1.2 OVERVIEW

Effective identity fraud control requires:

- clear governance – an explicit commitment by your organisation to effective identity fraud control, and a clear allocation of responsibilities;
- a sound appreciation of your organisation's exposure to the risks of identity fraud (including subsequent exposure for other organisations);
- sound systems and structures to:
  – prevent;
  – detect; and
  – respond to identity fraud;
- ongoing reviews of your organisation's risk exposure and mitigation efforts; and
- a responsiveness to emerging risks – a process for monitoring your identity fraud results against specified performance measures and, where required, adapting your fraud controls accordingly.

The Identity Fraud Management Framework

GOVERNANCE		
PREVENT	DETECT	RESPOND
PERFORMANCE MONITORING		
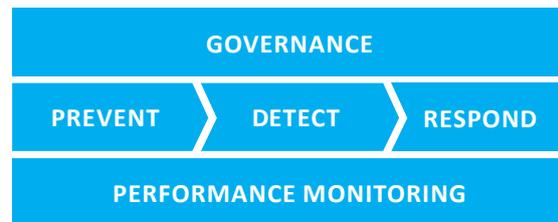
1.3 ROLES OF NEW ZEALAND AGENCIES

A number of New Zealand organisations have roles in preventing and managing the effects of identity fraud:

AGENCY	ROLE
Department of Internal Affairs	Provides overall leadership, including strategy, policy, services and standards for identity information.
	Authoritative source for most New Zealand citizens. Also holds identity information for many non-New Zealand citizens (e.g. marriage, death and name change information).
	Currently the Department has a number of information matching arrangements to support other agencies' identity verification processes and is developing a range of identity verification services that will help organisations to establish the identities of customers who are New Zealand citizens.
	www.dia.govt.nz
Department of Labour	Authoritative source for non-New Zealand citizens who visit or live in New Zealand.
	Operates VisaView, a visa verification service that enables employers to check immigrants' rights to work in New Zealand and is working to develop guidance and solutions to help organisations verify the identities of non-New Zealand citizens.
	www.dol.govt.nz
Insurance Council of New Zealand	Represents fire and general insurers in New Zealand. Members represent nearly all of New Zealand's general insurance businesses.
	www.icnz.org.nz
New Zealand Bankers' Association	Provides information and advice on banking and financial issues, such as the Code of Banking Practice.
	www.nzba.org.nz
New Zealand Police	Has a central role in identity fraud, including:
	• prosecution of criminal activities involving identity fraud; and
	• providing training in document examination techniques.
	www.police.govt.nz
Office of the Privacy Commissioner	Provides information and advice on privacy issues, such as data matching.
	www.privacy.org.nz
State Services Commission	Provides information on public service integrity and codes of conduct.
	www.ssc.govt.nz

2.0
GOVERNANCE ARRANGEMENTS

GOVERNANCE		
PREVENT	DETECT	RESPOND
PERFORMANCE MONITORING		
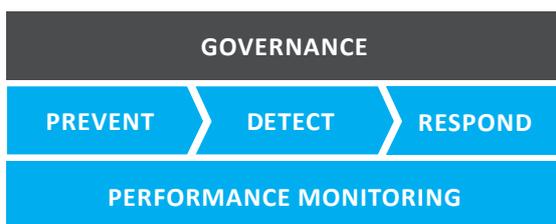
2.1 YOUR RESPONSIBILITIES

To deliver effective identity fraud control governance, your organisation needs to:

- have an understanding of its responsibility and accountability for identity fraud control and – reflecting this – appropriate internal governance arrangements (section 2.1.1);

- ensure clear leadership and a commitment to a highly ethical organisational culture (section 2.1.2);

- maintain effective relationships with other relevant organisations (section 2.1.3); and

- undertake comprehensive performance monitoring and review (section 2.1.4).

2.1.1 Taking responsibility within your organisation

It is important that you clearly identify the people within your organisation who are responsible for identity fraud controls. It is likely that responsibilities for identity fraud control will fall into several areas of an organisation.

For example, frontline processing staff, operational managers and investigation staff might be responsible for fraud detection controls, and business advisory and communications staff for fraud prevention controls. You need to review these responsibilities regularly as they are likely to change whenever you implement new controls or disestablish old ones.

Once you have identified the responsible people, you need to establish appropriate internal governance arrangements to manage the entire suite of controls efficiently.

Wherever possible, you should integrate your fraud control governance arrangements with your organisational governance framework. This will enable you to consider identity fraud control within the wider controls required to ensure the integrity, efficiency and cost-effectiveness of your business processes and services.

We also recommend that you make identity fraud control governance a specific area of responsibility in your organisational governance framework (i.e. as part of its terms of reference or through another mechanism that articulates the responsibilities of various governance groups). This will help to ensure visibility for identity fraud control in your organisation.

2.1.2 Leadership and commitment to a highly ethical organisational culture

Fraud control requires clear leadership and a commitment to a highly ethical culture from your chief executive and senior management personnel. This includes a commitment to effective systems for establishing and confirming identity in areas where your organisation is exposed to risk. (Sections 3 to 5 have more on the resources and approaches that will help you to implement and maintain such systems.)

All managers must demonstrate high standards of ethical behaviour – and ensure that their staff do so too. You can help to achieve this by establishing clear guidelines, then enforcing and communicating them effectively to your staff.

Commitment to a high standard of ethical behaviour starts from the top down

Connection

Responsibility

Communication

Values

Reward

Alignment

Clarity

Chief Executive

Senior Leadership Team

Managers and Team Leaders

Staff

2.1.3 Effective relationships with other organisations

Successful working relationships with other organisations allow you to draw on their expertise and knowledge, verify key identity information from the source and share your own knowledge of identity fraud.

For example, you could establish processes for verifying data with educational institutions and participate in shared services or work with New Zealand Police to identify and maintain lists of known fraudsters.

2.1.4 Performance monitoring and review

With an organisational commitment to monitoring performance, you will be able to determine the effectiveness of your identity fraud controls, and review your organisational identity risks and responses. (See section 3 for advice on periodic risk assessments and section 9 for more on monitoring performance.)

2.2 YOUR GOVERNANCE ARRANGEMENTS CHECKLIST

✓ Have you identified the people who are responsible for identity fraud control in your organisation?

✓ Do you have appropriate governance arrangements to support the ongoing management of your identity fraud controls, and any changes you make to them?

✓ Do you need to make any changes to your current governance arrangements to strengthen the focus on identity fraud control in your organisation?

✓ Does your organisation understand the roles of other organisations (section 1.3) that have an interest in identity fraud control?

3.0
RISK ASSESSMENT

GOVERNANCE		
PREVENT	DETECT	RESPOND
PERFORMANCE MONITORING		
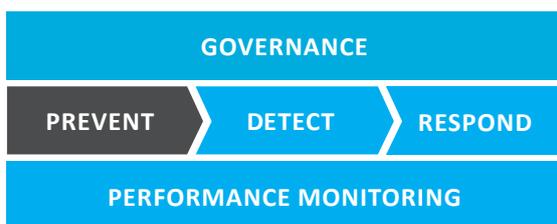
3.1 YOUR RESPONSIBILITIES

Undertaking risk assessments will enable you to understand the extent and nature of identity fraud within your organisation. It involves:

• assessing the risks for all your public-facing services, as well as the risks of staff recruitment/access to data scenarios (section 3.1.1); and

• taking a risk-based approach to allocating fraud prevention and detection resources (section 3.1.2).

3.1.1 Undertaking risk assessments

Recognising that you may already have your own risk management processes, the following guidelines are not intended to provide detailed information on risk management concepts or how to undertake risk assessments. They assume that your processes can be applied to a broad examination of identity fraud controls.

You need to make sure your approach is consistent with the risk assessment process in the Australian/New Zealand Standard *Risk Management* (AS/NZS 4360:2004)[6] and associated *Risk Management Guidelines* (SAA/SNZ HB 231:2004)[7], in addition to ISO 31000:2009, *Risk Management Principles and Guidelines.*[8] The Department of Internal Affairs' *Evidence of Identity Standard (EOI Standard*[9]*)* also provides extensive guidance on assessments of identity-related risks for services.

Your risk assessments should cover:

• all your public-facing services;

• any processes that involve personal information (e.g. human resources and payroll);

• your staff recruitment processes; and

• accessibility to data in your organisation.

You will also need to consider your overall risk appetite in these areas – that is, how much risk you are prepared to leave untreated to achieve cost savings or maintain convenience for your customers.

---

[6] **www.standards.govt.nz/default.htm** (for purchase)

[7] **www.standards.govt.nz/default.htm** (for purchase)

[8] **www.iso.org/iso/catalogue_detail.htm?csnumber=43170**

[9] **www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Evidence-of-Identity-Standard-Index or https://psi.govt.nz/evidence/default.aspx**

3.1.2 Adopting a risk-based approach

Fraud prevention and detection mechanisms can be costly to implement.

However, you do not need to use them everywhere in your organisation; instead, distribute them according to the level of risk (impact and likelihood) of fraudulent activities. With an understanding of your risk appetite and the distribution of risks in your organisation, you will be able to make informed decisions about allocating your resources.

(Sections 4 and 5 discuss fraud prevention and detection mechanisms and resources in more detail.)

3.2 YOUR RISK ASSESSMENT CHECKLIST

- ✓ Have you undertaken *EOI Standard* or equivalent risk assessments for all your public-facing services?
- ✓ Have you undertaken risk assessments for all data access scenarios?
- ✓ Do you understand your organisation's risk appetite?
- ✓ Have you decided how you will distribute your fraud prevention and detection efforts?

CASE STUDY: ANTI MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM LEGISLATION

The Anti-Money Laundering and Countering Financing of Terrorism Act 2009 takes a risk-based approach to financial transactions.

While it is acknowledged that all transactions will have some element of risk, the legislation differentiates between transactions requiring 'simplified', 'standard' and 'enhanced' customer due diligence. It places more emphasis on verifying customers' identities in more risky transactions.

For example, 'enhanced' customer due diligence is required when establishing a business relationship, conducting an occasional transaction or conducting a complex, unusually large transaction with a customer identified in the legislation as being more of a risk.

You can find more information about the Act in *Bell Gully's Practical Guide.*[10]

---

[10]**www.bellgully.com/resources/pdfs/Anti-Money-laundering-Countering-Financing-of-Terrorism-Bill-Jul09.pdf**

4.0
PREVENTION AND DETERRENCE CONTROLS

GOVERNANCE		
PREVENT	DETECT	RESPOND
PERFORMANCE MONITORING		
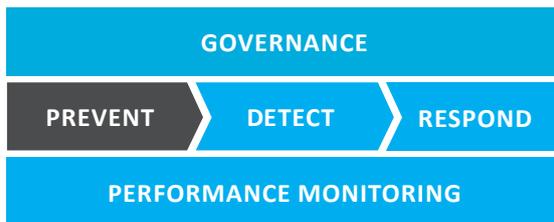
4.1 YOUR RESPONSIBILITIES

This section recognises that the most cost-effective way to control any crime is to prevent it occurring, as this avoids the costs to both victims and society. It provides guidelines for:

- developing internal controls for business processes that have identified vulnerabilities (section 4.1.1);
- developing 'deterrence controls', which convince potential fraudsters that fraud against your organisation is not worthwhile. Deterrence involves eliminating a fraud attempt that might otherwise occur:
  - deterrence controls for staff aim to create an anti-fraud culture through an emphasis on personal responsibility and ethical behaviour (section 4.1.2);
  - deterrence controls for the public aim to deter them from committing identity fraud. The controls focus mainly on increasing awareness of the consequences of committing identity fraud (section 4.1.3);
- developing 'preventive controls', which aim to stop attempted fraud happening or secure your organisation and processes against internal and external fraud;

- preventive controls for staff aimed at preventing them from committing fraud, including pre-employment screening (section 4.1.4); and
- preventive controls for the public aimed at preventing them from compromising their identities (section 4.1.5).

4.1.1 Internal controls

"Internal control was the most common method by which respondents detected their largest fraud covering nearly half (49%) of detected cases." [11]

Recognising that you probably already have internal controls and a formal internal control programme, this section does not provide comprehensive guidance on their design and implementation. Instead, it highlights some of the ways that you can use your internal controls to deter and prevent identity fraud.

Internal controls can be:

- manually based, where a person does something; or
- system enforced, where an operator is restricted by system controls to undertake only agreed tasks and activities.

Most business processes contain both manual and system-enforced controls. You need to choose which controls from the wide range available are most appropriate for your circumstances.

---

[11] KPMG's Fraud and Misconduct Survey 2010 www.kpmg.com/NZ/en/IssuesAndInsights/ArticlesPublications/Pages/Fraud-Survey-2010.aspx

Summary of the key types of internal controls applicable to identity-related business processes

INTERNAL CONTROL	DESCRIPTION
Policies and procedures	Policies and procedures should be: • developed for all business processes; • easily accessible for staff responsible for any aspect of a business process; and • kept current, with changes communicated to all relevant staff.
Communications	You should develop a coordinated communications plan for staff and customers.
Staff training	You should ensure that staff involved in any business process are properly trained in all aspects of their roles and organisational expectations. For identity fraud control, staff need training in: • the correct business processes for establishing and confirming customers' identities; • detecting possible incidents of customer identity fraud; and • detecting possible incidents of internal fraud.
Physical control	Establishing physical controls involves implementing security measures to deter or prevent unauthorised access to sensitive material. Examples include: • electronic access control systems (including magnetic swipe cards and biometrically enabled systems); • closed-circuit surveillance cameras; • motion or thermal alarm systems; • security guards; and • photo identity documents (e.g. employee cards).

Segregation of duties	Segregating the duties within a single business process makes it harder for individuals to circumvent policies and procedures. By allocating key duties and responsibilities among different staff members, you reduce the risks of error and internal fraud. In particular, you should separate responsibilities for: • recording identity information (i.e. data entry); • processing identity information (i.e. determining appropriate action); • authorising/approving identity information (i.e. approving the creation of a new identity record); and • review processes about information. To avoid the risk of collusion between individuals, monitor and be aware of potential breaches. Analysing actual versus expected results is one way to expose collusion.
Authority levels around decision-making	All decision-making, including any approvals, should be undertaken by staff with appropriate authority. If you are using electronic processes, these should be system enforced; for manual business processes, you will need to enforce your decision-making controls.
Auditing processes	Every internal control programme should include audits of processes – and ideally, a combination of routine and random auditing. Audit results should be reported to appropriate groups with responsibility for identity fraud control, and audit records of actions taken by staff in relation to business processes maintained.
Mystery shopping	'Mystery shopping' involves introducing dummy fraudulent or incomplete applications to business processes to test their ability to detect them. It can: • provide a valuable source of information on process deficiencies; • identify gaps in staff training programmes; and • help to raise and maintain staff awareness of identity fraud-related issues. Note that mystery shopping programmes need to be implemented with care (see the case study on page 15).
Access restrictions to personal data	Controlling access to personal data is a key internal control, whether the data is held electronically or in hard copy. Make sure you have processes to acknowledge staff changes quickly (e.g. when people change roles or leave your organisation).
Fraud hotlines	Anonymous channels for whistle-blowing provide staff and the general public with confidence to report inappropriate or illegal behaviour. Ensure you undertake appropriate investigative processes before accepting anonymous tips.

Developing an internal controls programme

A series of internal controls can apply to a single business process (e.g. establishing a new customer's identity) or for multiple business processes.

For this reason, you need to develop your internal controls at both organisational and business process levels. They should cover not only system, but also people-related integrity.

When developing internal controls for a business process you need to:

- define the business process;
- establish its objectives, particularly in terms of identity fraud control;
- determine the internal controls required to support the business process, and their objectives (control objectives);
- design, in detail, the control tasks and activities;
- identify and devise monitoring arrangements for the risks associated with the controls;
- establish how you will report on the control tasks and activities, and progress in achieving the control objectives; and
- design the processes required to modify existing internal controls (where necessary) in response to current, changed or new processes and risks.

Implementing internal controls can impose both internal and external costs, so ensure the controls are proportionate to the risks, while enabling your organisation to meet your customers' needs. You also need to make sure you apply the controls consistently for maximum effectiveness.

CASE STUDY: MYSTERY SHOPPING

In March 2009, the United States Government Accountability Office (US GAO) reported that it had conducted undercover tests of the US passport issuing system.

The investigator managed to obtain four genuine passports using fraudulently obtained or counterfeit documents. In one case, the passport was obtained using the genuine social security number of a five-year-old child, despite the accompanying application giving his age as 53 years.

The exercise was repeated in 2010, with five out of seven fraudulent applications leading to passports being issued. Two were later recalled when fraud was detected.

What did this achieve?

- It led to corrective actions and the US GAO recommended further work to improve passport systems.
- The 2010 exercise identified new issues and interventions that had been successful but implemented too late in the process.

Other mystery shopping scenarios

This case study is about mystery shopping directed at identifying system holes and failures. You could also use mystery shoppers to identify staff problems, such as in the messages given to customers, information provided and whether bribes are accepted.
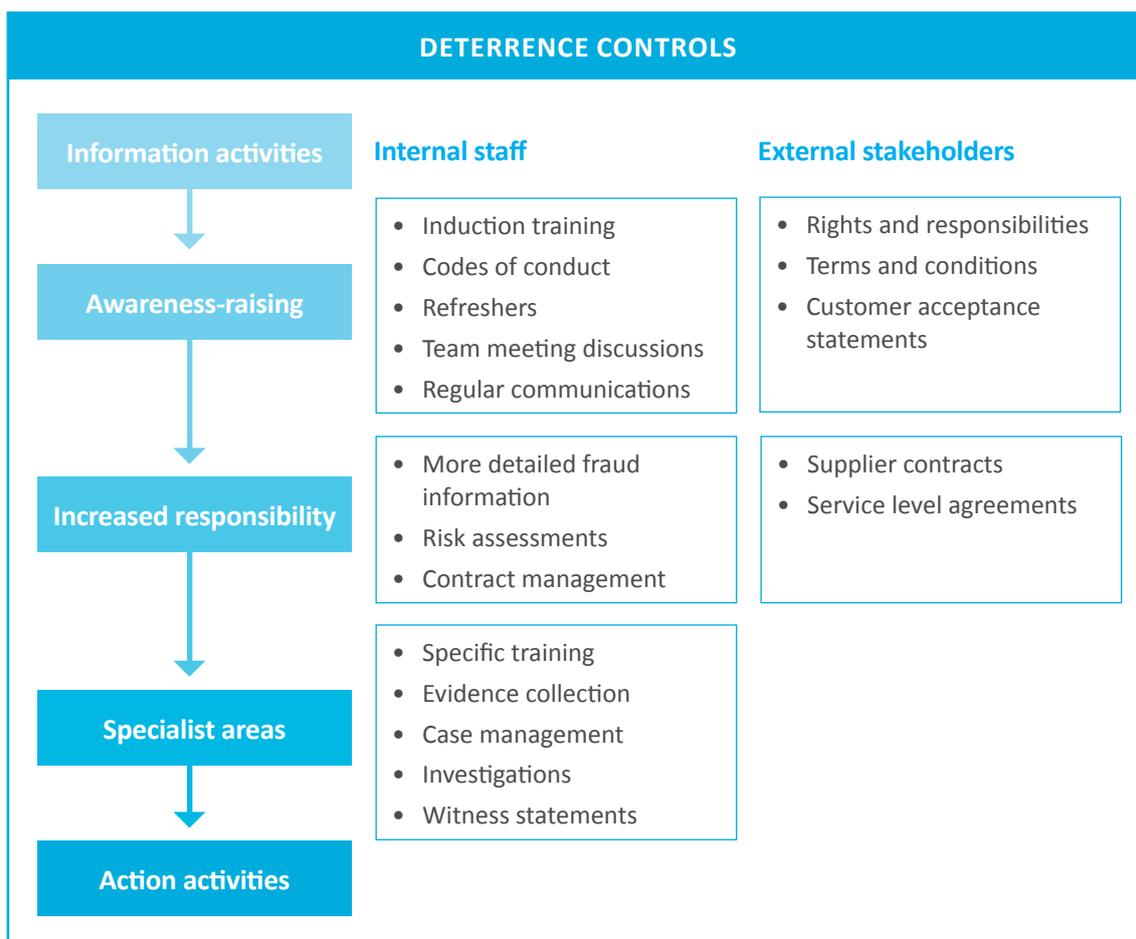
4.1.2 Deterrence controls for staff

Deterrence controls involve providing information to employees and customers on fraud you have detected and the actions you have taken – giving a clear illustration of the serious consequences of this crime. The most important fact about deterrence is that it derives from perceived risk and not actual risk.

The information can be disseminated through various forms, including awareness-raising, training and external communications.

Awareness-raising and training

Awareness-raising and training are effective methods for ensuring that all staff are aware of their responsibilities for identity fraud control and ethical behaviour. We recommend strong induction processes and ongoing training.

Staff working in areas with a higher risk of identity fraud may need more detailed training than general awareness-raising, while those responsible for investigations will require specific training.

DETERRENCE CONTROLS		
Information activities ↓ **Awareness-raising** ↓ **Increased responsibility** ↓ **Specialist areas** ↓ **Action activities**	**Internal staff** • Induction training • Codes of conduct • Refreshers • Team meeting discussions • Regular communications • More detailed fraud information • Risk assessments • Contract management • Specific training • Evidence collection • Case management • Investigations • Witness statements	**External stakeholders** • Rights and responsibilities • Terms and conditions • Customer acceptance statements • Supplier contracts • Service level agreements

Strategies to raise awareness include:

- circulating identity fraud control plans and/or policies;
- induction and ongoing refresher training about identity fraud control;
- putting messages on screensavers or alerts; and
- publicising the issue in employee newsletters, intranet articles and emails.

Identity fraud awareness-raising training should cover:

- definitions of identity fraud and related terms;
- ethical behaviour requirements of all staff (whether they are on permanent or fixed-term contracts or are temporary employees, consultants or contractors);
- your organisation's identity fraud policy statement (or fraud policy statement) and identity fraud control policy;
- things to watch for that could indicate someone is attempting, or has committed, identity fraud;
- what to do if you suspect identity fraud;
- customer service training; and
- responsibility for handling allegations and cases of identity fraud and code of conduct breaches.

A number of sector-specific organisations provide guidance on ethical behaviour. In the public sector, the State Services Commission provides information on state servant integrity and *Codes of Conduct,*[12] while the New Zealand Bankers' Association has a *Code of Banking Practice*[13] for the finance sector.

4.1.3 Deterrence controls for the public

"The most effective strategies designed to change attitudes rely on motivations rather than fear. They aim to persuade people of the undesirability of a particular behaviour. Attitude changing strategies rely to a large extent on publicity campaigns to achieve their effect so it is important that departments carry out a full appraisal of the benefits of any proposed advertising campaign and to establish some way of measuring the outcomes of such campaigns."[14]

General publicity about the consequences of identity fraud is an important control measure. It should include:

- warnings on all paper, electronic and online forms and in face-to-face customer interactions with potential identity-related risks; and
- educating the public by highlighting successful prosecutions involving identity fraud. This demonstrates the consequences of the crime.

....

[12] **www.ssc.govt.nz/display/document.asp?navid=296**

[13] **www.nzba.org.nz/banking-standards/code-of-banking-practice/**

[14] *From Managing the Risk of Fraud – A Guide for Managers* **www.hm-treasury.gov.uk/d/managing_the_risk_fraud_guide_for_managers.pdf**

11 Your Applicant Declaration

Tick one box

☐ I have completed this application in my own handwriting.

☐ Someone else has filled in this application for me because I have a disability or language difficulty.

If someone else has filled in this application for you but you are able to sign your own name, you must sign this section. If you are unable to sign your own name, the signature in this section must be left blank. The person who filled in the application form for you must not sign this section but must sign the statutory declaration in section **D**.

▶ I declare that the information I have given in this application is, to the best of my knowledge, true, complete and correct.

▶ I understand that if I have provided false information my passport can be cancelled and I can, by law, be fined or imprisoned.

▶ I confirm that I have read the section relating to Privacy in the Guide Notes for this application.

▶ I agree that, for the purposes of this application, other government agencies may release personal information about myself which will assist the Passport Office in determining my entitlement to be issued with, or continue to hold, a New Zealand Passport.

▶ I understand that if I use, or have possession of, a forged or false New Zealand travel document, I may be liable on conviction to imprisonment for a term not exceeding 10 years, a fine not exceeding NZ$250,000.00, or both.

WARNING It is an offence against the Passports Act 1992 to knowingly or recklessly make a statement that is false or misleading in a material particular for the purposes of gaining a New Zealand Passport.

Sign your Applicant Declaration here

Date signed

Warnings on forms

Warnings on forms should be tailored to the particular service and include statements about:

- the consequences of providing false information, including specific legislation under which offences can be prosecuted and the penalties that can apply; and

- providing consent for personal information to be shared with other organisations to establish identity or entitlement information.

Above is an example of a warning, from the Department of Internal Affairs' passport application form.

Public education

The Department of Internal Affairs is coordinating a cross-government communications strategy for raising public awareness of identity issues. If your organisation would like to be involved, or would like information on key messages for customers, contact the Department of Internal Affairs at ICCP@dia.govt.nz.

4.1.4 Prevention controls for staff

Prevention controls for staff can apply:

- before they start working for you (through pre-employment screening); and
- after they start working for you (for example, through access controls, segregation of duties, and physical security).

Pre-employment screening

Robust pre-employment screening helps to reduce the likelihood of identity fraud activities among staff members, among other things. Employing the 'right' staff is an effective control measure and ethical behaviour is critical.

You can find helpful guidance on pre-employment screening in the *EOI Standard* and the United Kingdom's *Baseline Personnel Security Standard*,[15] which covers public sector workers. The *Good Practice Guide on Pre-Employment Screening*[16] by the UK Centre for the Protection of National Infrastructure is suitable for use in both the public and private sectors.

Your pre-employment screening process should:

- start with a robust candidate identity verification check (including a police check);
- verify the candidate's employment history and qualifications or professional registrations;
- include referee checks and verify that referees are genuine and in a position to provide references;
- check the candidate's 'right to work' status (their citizenship or immigration status, age and any medical checks required for certain professions) (see case study: VisaView);
- check for any criminal record;

- check that behavioural examples provided at interviews are true and correct; and
- other checks – an assessment of items and responses that do not "feel right" that may increase risk e.g. academic achievement above the role, extended periods of unemployment, quality of application exceeding standard for role and/or not consistent with other communication with applicant.

CASE STUDY: VISAVIEW

Since August 2010, the Department of Labour has been operating VisaView, a visa verification service that allows New Zealand employers to check whether a person who is not a New Zealand citizen can work in New Zealand for that employer. It also enables registered employers to confirm New Zealand passport information provided by jobseekers, and therefore confirm New Zealand citizenship and entitlement to work in any job.

As of March 2011, 1300 employers have registered with the service.

Further information about the service, including a "how to use" video tutorial can be found on the VisaView homepage (www.immigration.govt.nz/community/stream/visaview).

---

[15] **www.cabinetoffice.gov.uk/media/45160/hmg_bpss.pdf**

[16] **www.cpni.gov.uk/Docs/Pre-employmentscreening.pdf**

Pre-employment screening

	IDENTITY ESTABLISHMENT CHECKS	
Employment History Verification		Right to Work

Job Specific Checks

Financial/Credit History	Personal Background	Criminal Checks
Security Clearance	Psychometric/Integrity and Skills Testing	Health
	Qualifications	Professional Registrations
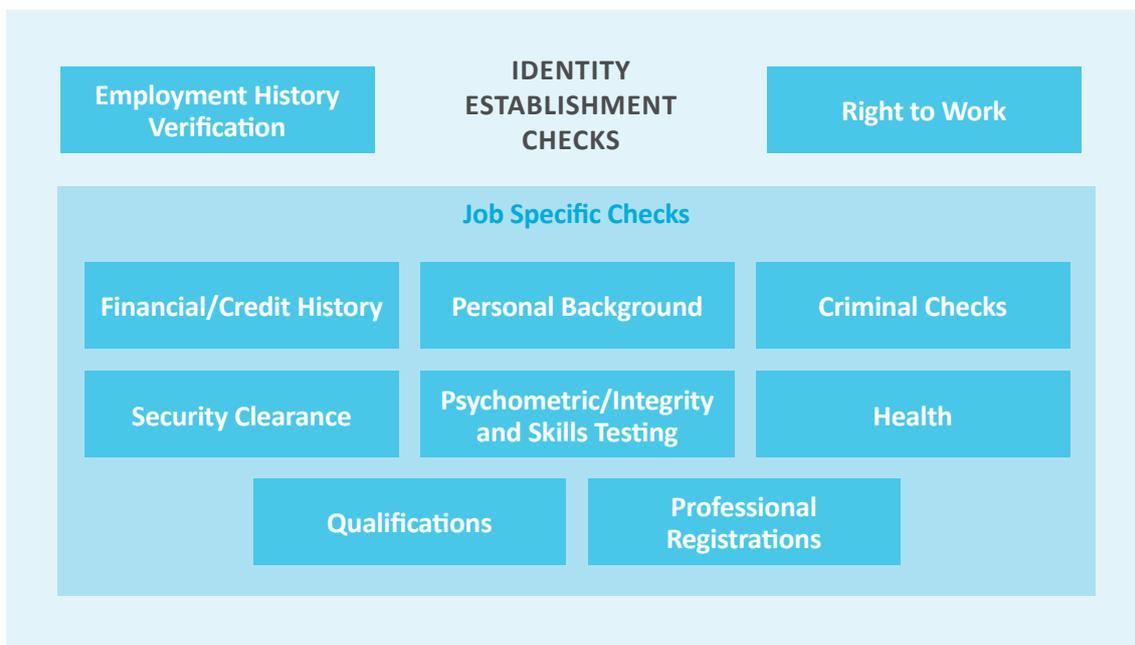
CASE STUDY: LISA CLEMENT

In November 2000, the Ministry of Social Development employed Lisa Clement (aka Lisa Donnelly) as an executive assistant to a Work and Income New Zealand manager, who was responsible for finance. Clement later picked up responsibility for contracts and payments.

Three years later, a manager found a forged invoice bearing his name on the photocopier and investigated. Clement had been using her position and knowledge to manipulate invoices, payments, budgets and forecasting to defraud WINZ of almost $2 million.

Clement had previous criminal convictions for dishonesty offences and had also been bankrupted twice. She failed to declare the bankruptcies and convictions on her application form, gave a false date of birth and added a middle name to her name.

How did this happen?

- An inadequate identity check formed the basis for all further background checks. If Clement's identity had been established, her background checks would have highlighted her past.

What else can happen?

- People can get jobs that enable them to access sensitive information or things that can be sold or used for personal benefit.
- People with pasts they wish to hide can falsify their identities.
- People who do not have the qualifications they claim can gain positions fraudulently.

4.1.5 Prevention controls for the public

"It is always possible to have controls that prevent fraud, but such controls need also to enable departments to give a timely service to honest customers, without unacceptable burdens. Designing effective controls depends on understanding the scale and nature of the risks and the costs." [17]

There are a number of things that members of the public can do to help prevent identity theft. You can help by providing advice on:

- safeguarding identity information and documents;
- how to detect potential identity theft early; and
- steps to take if your identity has been compromised.

A number of organisations (both public and private) have campaigns targeting public awareness on related issues. These include:

- the Ministry of Consumer Affairs – *Scamwatch*;[18]
- the Department of Internal Affairs – *Anti-Spam*;[19]
- the Office of the Privacy Commissioner – *Privacy Awareness Week*;[20] and
- *National Identity Fraud Awareness Week*,[21] which is run by a consortium of private sector companies: Norton, Fellowes, Veda Advantage and Secure Identity.

The cross-government public awareness strategy for identity issues has key messages for the public on keeping their identity safe and responding if they become victims of identity theft. For more information, contact the Department of Internal Affairs at ICCP@dia.govt.nz.

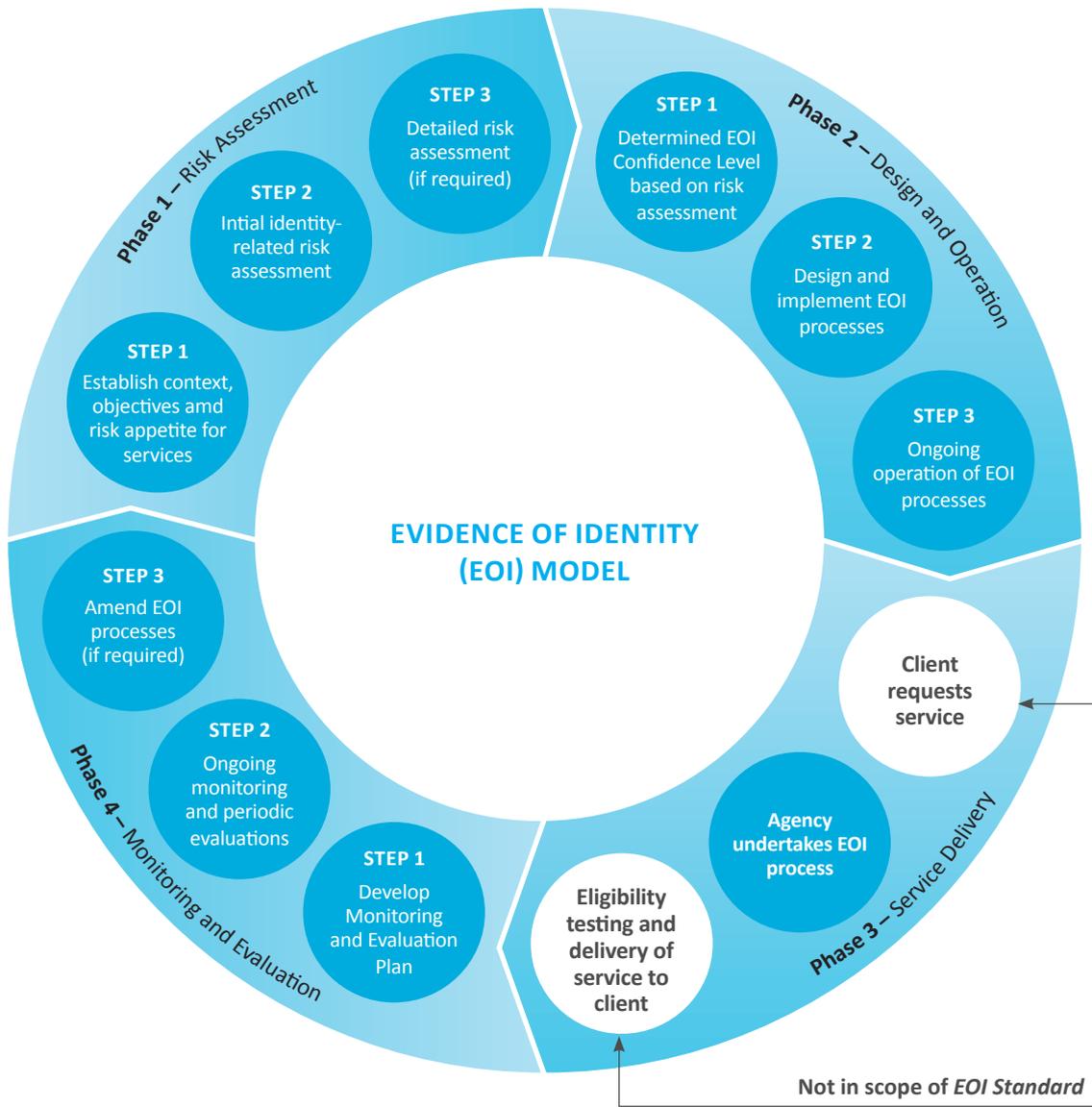[17] Caroline Mawhood, Assistant Auditor General, UK National Audit Office, Tackling External Fraud, June 2008 **www.nao. org.uk/guidance__good_practice/acquisitions-1/fraud_and_ corruption.aspx**

[18] **www.consumeraffairs.govt.nz/scams/about-scamwatch**

[19] **www.dia.govt.nz/Services-Anti-Spam-Index**

[20] **http://privacy.org.nz/privacy-awareness-week/**

[21] **www.stopidtheft.com.au/**

EVIDENCE OF IDENTITY (EOI) MODEL

Phase 1 – Risk Assessment

STEP 1
Establish context, objectives amd risk appetite for services

STEP 2
Intial identity-related risk assessment

STEP 3
Detailed risk assessment (if required)

Phase 2 – Design and Operation

STEP 1
Determined EOI Confidence Level based on risk assessment

STEP 2
Design and implement EOI processes

STEP 3
Ongoing operation of EOI processes

Phase 3 – Service Delivery

Client requests service

Agency undertakes EOI process

Eligibility testing and delivery of service to client

Not in scope of *EOI Standard*

Phase 4 – Monitoring and Evaluation

STEP 1
Develop Monitoring and Evaluation Plan

STEP 2
Ongoing monitoring and periodic evaluations

STEP 3
Amend EOI processes (if required)

Establishing and confirming identity

Successful identity fraud prevention relies on having processes to establish a person's identity and subsequently confirm the identity in future transactions.

Establishing identity

It is vitally important to establish people's identities accurately, and to have effective processes for doing so.

Processes that can be circumvented provide an easy avenue for creating false identities – and once these false identities have been accepted as genuine, subsequent interactions also become easy. Any credentials issued by the identifying organisation can be used to establish false identities with others.

All organisations that deliver services to the public containing identity-related risks should use the *EOI Standard.* Part of the *New Zealand E-Government Interoperability Framework (e-GIF)*[22] authentication standards, it provides guidelines for establishing and confirming people's identities.

While written predominantly for the public sector, these standards are also useful for the private sector.

To the left is an overview of the steps required to implement EOI processes for services that require people's identities to be established.

Subsequent confirmation of identity services

Once a customer's identity has been established, they are likely to go on to interact with other organisations. The challenge is to develop cost-effective business processes that continue to link them correctly to an established identity record.

In most cases this will require identity confirmation through channels such as:

- the Internet;
- telephones;
- personal interactions;
- mail; and
- email.

....

[22] **www.e.govt.nz/standards/authentication**

The standards and documents that make up the suite of e-GIF authentication standards

STANDARD/DOCUMENT NAME	PURPOSE
Guide to Authentication Standards for Online Services	Provides a high-level overview of the New Zealand e-GIF authentication standards.
Evidence of Identity Standard	Specifies a business process for establishing and confirming the identities of government agency customers. Applies to services delivered through both offline and online channels.
Authentication Key Strengths Standard	Specifies the authentication keys to be used for online authentication and the protections necessary for the authentication exchange.
Data Formats for Identity Records Standard	Specifies data formats for a set of customer information data elements that government agencies can use in customer identity records.
Password Standard	Specifies requirements for passwords used for online authentication.
New Zealand Security Assertion Messaging Standard	Specifies messaging standards for communication authentication assertions.
Guidance on Multi-Factor Authentication	Provides an overview of multi-factor authentication. May be superseded once other authentication key standards have been developed (not a New Zealand e-GIF standard).
Security Assertion Messaging Framework	Provides a general introduction for security assertion messaging (not a New Zealand e-GIF standard).

Online reconfirmation

The Authentication Standards (of which the *EOI Standard* is a part) explain in detail the requirements for online identity confirmation (e.g. using a PIN). They also describe the combinations needed to meet different risk levels of identity confirmation, and provide good practice advice on the use of the different solutions (e.g. the minimum requirements for effective passwords).

Offline reconfirmation

The *EOI Standard* deals with offline reconfirmation. Note that not all channels are created equally, and one channel might be more suited to a business process requirement than another.

When choosing the channel(s) for your own organisation, you should consider carefully how much confidence you need when reconfirming a person's identity. For example, people reapplying for passports do not need to prove their identities to download the form.

4.2 YOUR PREVENTION AND DETERRENCE CONTROLS CHECKLIST

✓ Does your organisation screen job applicants to ensure they are who they say they are and have an understanding of the importance of integrity?

✓ Do you have an anti-fraud culture in which staff understand the standards of conduct required, and their personal responsibilities for reporting suspected cases of identity fraud (either by customers or involving staff)?

✓ Do you send a strong message to potential fraudsters that they are likely to be caught and punished? For example, do you create press releases on people or businesses prosecuted or run any targeted or wider campaigns regionally/nationally?

✓ Do you seek to influence customers' and the wider general public's attitudes to identity fraud?

✓ Do you build identity fraud controls into any new programme that delivers benefits to the public?

✓ Have you reviewed your business processes for establishing customers' identities against the *EOI Standard?*

5.0
DETECTION METHODS

GOVERNANCE		
PREVENT	DETECT	RESPOND
PERFORMANCE MONITORING		
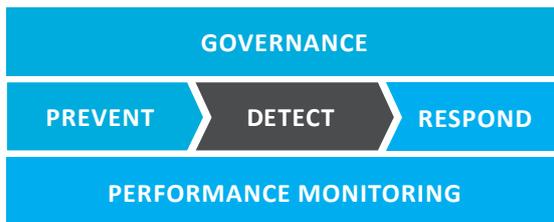
5.1 YOUR RESPONSIBILITIES

This section provides guidelines for:

- staff detection of fraud through routine process checks (section 5.1.1);
- using risk profiles (section 5.1.2);
- using biometric recognition technology (section 5.1.3);
- enabling members of the public to contact your organisation about suspicions (e.g. through telephone hotlines) (section 5.1.4);
- data matching (section 5.1.5); and
- data mining (section 5.1.6).

5.1.1 Routine process checks

Routine process checks by staff are a particularly important fraud detection method, especially when part of your processes for establishing and confirming people's identities.

5.1.2 Risk profiles

The *EOI Standard* defines risk profiling as "the process of gathering data on characteristics (e.g. customer behaviours) in order to identify categories of risk".

Risk profiling is potentially useful in detecting identity fraud, particularly as part of routine application processing. It will help your organisation to identify situations with a higher likelihood of attempted identity fraud, and where additional checks or investigation may be required.

Risk profiling involves:

- using information your organisation has collected about previous cases where misuses or abuses of identity (or other types of crime) were detected; and
- using information from other sources, including government agencies, overseas counterparts and other intelligence sources, to highlight characteristics that are more likely to involve identity fraud.

Ideally, a risk profile should prioritise people or applications deemed to be more likely to be fraudulent than an average selection, which therefore warrant closer investigation. It will help you to target resources more proactively, rather than relying on a third party (e.g. another organisation or member of the public) to provide information about possible false identities. Risk profiles should be subject to review and change over time.

5.1.3 Biometric technologies

Appropriate use of biometric technologies

Collecting biometrics[23] and then using biometric recognition technologies provides a powerful means for detecting potential identity fraud. However, biometric recognition technologies are still maturing, and are relatively complex and expensive to implement.

Biometric technologies are generally most appropriate when there is a relatively high level of identity-related risk involved in establishing or subsequently confirming identity.

In the public sector the Cross Government Biometrics Group has developed *Guiding Principles for the Use of Biometric Technologies for Government Agencies.*[24] While these principles are targeted at the public sector, some may also be relevant for the private sector.

....

[23]A biometric is the measurement of a unique physiological or behavioural characteristic. Physiological characteristics include face, fingerprint, iris, palm and DNA. Behavioural characteristics include voice, keystroke, signature and gait

[24]**www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Guiding-Principles-for-the-Use-of-Biometric-Technologies-Index?OpenDocument or https://psi.govt.nz/biometrics/default.aspx**

CASE STUDY: WAYNE PATTERSON

In September 2006, the Ministry of Social Development was contacted by a bank about suspicious activity in a number of accounts that were receiving benefits. When the Ministry checked its system, it discovered 123 false identities.

Wayne Patterson had created high-quality false birth certificates and used them to obtain secondary identification, such as a driver licences. He then claimed superannuation and at the height of his offending was being paid $56,000 a fortnight. In total, he defrauded the Ministry of $3.4 million.

How did this happen?

• Lack of data checking between the Ministry of Social Development and other government departments.

• Inadequate data mining by the Ministry.

• The ease of gaining other identification with a false birth certificate.

How could it have been prevented?

The Department of Internal Affairs' Data Validation Service would have prevented the fraud occurring by checking the birth certificate data against the Department's records; its fictitious nature would have been discovered.

More frequent data mining for similarities between beneficiaries would have exposed the offending earlier.

The table below summarises different ways that biometric technologies can be used to detect potential identity fraud

MATCHING	COMMENT
1-to-many matching	This involves taking biometric information (for a particular type of biometric) collected from an individual and comparing it with all other biometric information held by your organisation to detect any potential matches.
	1-to-many matching is primarily used to detect a single person's attempt at creating multiple identity records using differing biographical information. It is particularly suited to the initial establishment of identity.
1-to-1 matching	This involves taking the biometric information (for a particular type of biometric) collected from an individual and comparing it with biometric information you have already collected for the initial establishment of the claimed identity.
	1-to-1 matching is primarily used to detect attempted impostor fraud (i.e. someone different from the established identity trying to pass themselves off as that person). It is most suitable for subsequent confirmations of identity.
1-to-some matching (watchlists)	This involves taking the biometric information (for a particular type of biometric) collected from an individual and comparing it with the biometric information of selected individuals that pose a particular risk (e.g. known identity fraudsters or criminals). This is often referred to as matching against a watchlist.
	1-to-some matching is used primarily to detect individuals who pose a particular risk.
Many-to-many matching	This involves comparing biometric information (for a particular type of biometric) of a database against all other records in the database. It is effectively multiple 1-to-many tests.
	Many-to-many matching is used primarily to cleanse a database of old, possibly fraudulent/multiple identities. It is often repeated as matching algorithms' performance improves (e.g. the ability to match people wearing glasses successfully).

5.1.4 Fraud hotlines

Fraud hotlines are a useful way for both staff and members of the public to give information anonymously about possible fraud cases. A New Zealand example is *Crimestoppers*,[25] through which members of the public provide information to New Zealand Police without divulging their personal details.

Fraud hotlines are cost-effective, as they can be as simple as a dedicated email account or an online form that emails the details to a set destination. They can also be set up to be anonymous through simple mechanisms such as a drop box or free phone number.

When implementing a fraud hotline, it is important to advertise extensively its availability, contact details and confidential nature.

CASE STUDY: FRAUD HOTLINES

Statistically, tip-offs are one of the most common ways to detect fraud.

Although most people would hope they would do the right thing if they uncovered a co-worker or friend committing fraud, tip-offs are often delayed for fear that the perpetrator will discover who blew the whistle. Anonymous fraud hotlines are increasingly popular, and can be run centrally within industries (e.g. the Insurance Council), by an organisation itself (e.g. Waikato District Health Board) or via an external independent provider (e.g. Report-it-Now).

5.1.5 Data matching

Data matching is an electronic check of one set of data against another, and is commonly used to find records in both sets of data that belong to the same person.

It can be used to check for fraud – for example, in comparing a list of people receiving monetary benefits with a list of people who are imprisoned, or comparing Ministry of Justice and Customs' data to identify serious fine defaulters crossing the border.

To help users to focus their resources on matches where fraud is most likely, data-matching software can:

- highlight the highest priority matches;
- enable users to filter only those matches that meet investigators' criteria; and
- explain the importance of each match type and protocols for sharing information between organisations to investigate the suspected fraud.

Data matching can be privacy invasive, so you should undertake it only when allowed by legislation and in consultation with the Office of the Privacy Commissioner.[26]

5.1.6 Data mining

Data mining involves checking data for similarities that could indicate fraud. It is useful in detecting identity fraud and establishing whether someone committing fraud has more identities than those discovered through other techniques.

Data mining software checks large amounts of data for similarities and patterns that might not become apparent using another technique. The Ministry of Social Development used it as part of the investigation into Wayne Patterson's fraud (the case study in section 5.1.3). It revealed that he had 123 identities, all receiving benefits.

You should implement data mining software carefully, because its usefulness can be affected by many factors, including insufficient sample sizes.

5.2 YOUR DETECTION METHODS CHECKLIST

✓ Does your organisation make routine process checks?

✓ Do you use risk profiles and data mining – and if not, could they be useful options?

✓ Do you use biometric recognition technology – and if not, could it be integrated into current systems?

✓ Do you use hotlines? If yes, could they be expanded or, if not, set up?

✓ Do you use data matching with an authoritative data source (allowed for under legislation)?

---

[25] **www.crimestoppers-nz.org**

[26] **www.privacy.org.nz/data-matching-introduction**

6.0
INVESTIGATING IDENTITY FRAUD

GOVERNANCE		
PREVENT	DETECT	RESPOND
PERFORMANCE MONITORING		
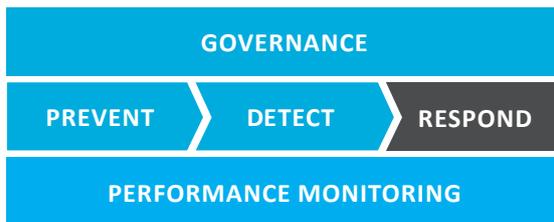
6.1 YOUR RESPONSIBILITIES

This section provides guidelines on:

- selecting cases for investigation (section 6.1.1);
- best practice for investigation processes (section 6.1.2); and
- training requirements and standards for investigators (section 6.1.3).

6.1.1 Selecting cases to investigate

In many cases, identity fraud is a precursor to other crime including general fraud and it is through investigating the general fraud that identity fraud is uncovered. In this sense identity fraud can be seen as a subset of general fraud and much of the investigation relating to identity fraud will have been covered by general investigative fraud procedure.

While it is important to investigate every case of suspected identity fraud, your organisation might not be able to respond to each case immediately (perhaps owing to limited resources). In this case, you need to decide which cases of suspected fraud you will investigate with a view to prosecution, with the remainder subject to some other form of sanction.

Effective sanctions can do more than simply punish the individual: they have wider deterrent impacts and should encourage the non-compliant to return to compliance. Visible sanctions that work can also reinforce the perception among compliant individuals that the system is fair.

The three classes of fraud described by the 2006 UK Fraud Act could be useful when applied to identity fraud:[27]

- fraud by false representation;
- fraud by failing to disclose information; and
- fraud by abuse of position.

---

[27]**www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060035_en.pdf**

6.1.2 Investigation processes

You will need to create an investigative process that works with the information you have available and within your business context.

Managing the Business Risk of Fraud: A Practical Guide[28] suggests a number of activities for investigating general business fraud, which can also be used for identity fraud:

- categorising issues;
- confirming the validity of the allegation;
- defining the severity of the allegation;
- escalating the issue or investigation when appropriate;
- referring issues outside the scope of the programme;
- conducting the investigation and fact-finding;
- resolving or closing the investigation;
- listing types of information that should be kept confidential;
- defining how the investigation will be documented; and
- managing and retaining documents and information.

If an investigative process for general fraud precludes the discovery of identity fraud (see section 6.1.1), some of the activities for investigating identity fraud might have already happened.

6.1.3 Training requirements and standards for investigators

Your investigators should be given comprehensive training on the investigative approach, collating evidence, legal aspects and putting together a prosecution case.

This training is likely to include membership of professional groups, which enables investigators to increase their knowledge and skills through shared experiences and expertise. The Department of Internal Affairs' *National Compliance Qualifications Project,*[29] which is part of the Compliance Common Capability Programme, will include a framework of three separate qualifications for people working in the compliance area.[30] It is due to be registered with the New Zealand Qualifications Authority by late 2011.
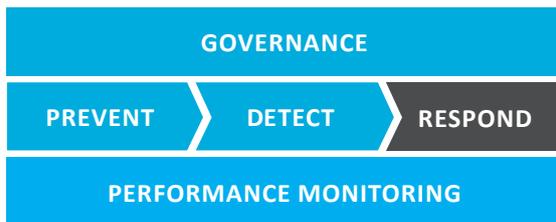
The other main project in the Compliance Common Capability Programme is the *Guide to Effective Compliance Organisation Design,* which should also be available in 2011.

6.2 YOUR IDENTITY FRAUD INVESTIGATION CHECKLIST

✓ Does your organisation have clear guidelines for investigators on the types of case to progress to investigation?

✓ Do you have performance measures for investigations?

✓ Do you have good training regimes for investigators and clear, practical standards for them to follow?

---

[28]**http://fvs.aicpa.org/NR/rdonlyres/98BD10EC-CC12-4D14-848D-E5BDB181F4EE/0/managing_business_risk_fraud.pdf**

[29]**www.learningstate.govt.nz/upload/downloadable_files/Learning_State_Compliance_Project.pdf**

[30]Compliance is defined as "the process of ensuring that people adhere to rules and regulations"

7.0
IDENTITY RESTORATION

GOVERNANCE

PREVENT	DETECT	RESPOND

PERFORMANCE MONITORING

7.1 YOUR RESPONSIBILITIES

This section covers:

- how your organisation can help people who are the victims of identity theft to regain their identities (section 7.1.1); and
- other agencies involved (Police and the Department of Internal Affairs).

7.1.1 Support for identity restoration

Identity theft might only be detected when the true owner of the identity applies for a service.

It is important to remember that identity theft can be extremely stressful for the victim. Doing everything you can to help will go a long way towards reducing this stress and help the victim to restore their identity as quickly as possible.

If someone contacts your organisation about misuse of their identity, you need to:

- provide them with the checklist developed by the Department of Internal Affairs (and available from ICCP@dia.govt.nz), which provides a step-by-step guide to the process they should follow and who can help them along the way;
- advise them that they must contact New Zealand Police, then any other appropriate organisation identified in the checklist;
- add a note to their file, if appropriate; and
- ensure that no further misuse can happen.

7.2 YOUR IDENTITY RESTORATION CHECKLIST

✓ Does your organisation have a process to prevent further misuse of a person's identity once you know they have been a victim of identity theft?

✓ Do you have guidelines to help victims of identity theft?

8.0
PROSECUTING IDENTITY FRAUDSTERS

GOVERNANCE		
PREVENT	DETECT	RESPOND
PERFORMANCE MONITORING		
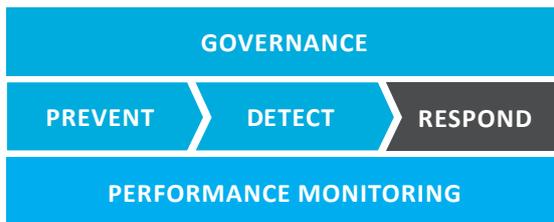
8.1 YOUR RESPONSIBILITIES

This section provides guidelines for:

- selecting cases to progress to prosecution (i.e. balancing the costs and benefits of prosecution) (section 8.1.1);
- supporting legislation, penalties and fines (section 8.1.2); and
- recovery and restitution (section 8.1.3).

8.1.1 Selecting cases to progress to prosecution

Referring cases to law enforcement agencies for prosecution can take a long time and involve significant resources. We recommend that you consider the *Crown Law Prosecution Guidelines*[31] as part of each decision.

You could also refer to the UK National Audit Office's *Tackling External Fraud,*[32] which suggests that you consider:

- whether you have enough evidence to obtain a conviction;
- whether the case involves a systematic attack on your organisation's systems and has led to substantial amounts of money being lost;
- whether there is a history of re-offending;
- whether professionals such as lawyers and accountants are involved in the fraud; and
- whether prosecution will increase the deterrent effect.

8.1.2 Supporting legislation, penalties and fines

Your organisation needs to have good knowledge of the supporting legislation under which you can prosecute and the penalties/fines involved. This applies whether you are prosecuting under general legislation (e.g. the Crimes Act 1961) or specific legislation, such as the Passports Act 1992.

8.1.3 Recovery and restitution

Fines and other penalties will only be effective deterrents if you act promptly to enforce them. Make sure you monitor the progress of fine payments; if the fines cover your investigation costs, you might have more scope to investigate fraud.

8.2 YOUR PROSECUTION CHECKLIST

- ✓ Does your organisation use guidelines to choose cases for prosecution?
- ✓ Are the penalties in the legislation under which your organisation operates sufficient to deter offenders?
- ✓ Do you have processes to recover any fines or penalties imposed by the courts?

---

[31]**www.crownlaw.govt.nz/uploads/prosecution_guidelines.pdf**

[32]**www.nao.org.uk/guidance__good_practice/acquisitions-1/ fraud_and_corruption.aspx**

9.0
PERFORMANCE MEASURES AND MONITORING

GOVERNANCE		
PREVENT	DETECT	RESPOND
PERFORMANCE MONITORING		
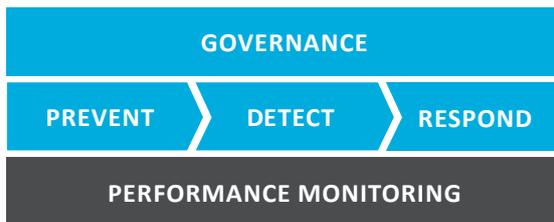
9.1 YOUR RESPONSIBILITIES

This section provides guidelines on:

- performance measures you can use to establish the effectiveness of your identity fraud controls (section 9.1.1); and

- if you are a government agency, the requirements to report on your identity fraud performance measures to the Department of Internal Affairs (section 9.1.2).

9.1.1 Performance measures

Performance measures are recommended for each of the areas in the identity fraud control management framework.

Performance monitoring and risk assessments are closely linked: risk assessments help to identify vulnerabilities that need addressing, while performance monitoring determines the ongoing effectiveness of your identity fraud controls. Where possible, you should develop performance measures for assessing the effectiveness of identity-related risk mitigations.

Managing the Business Risk of Fraud[33] suggests a number of measures your organisation could use to monitor your ongoing performance and the effectiveness of general fraud controls. Note that while they have been developed for general fraud, they are also applicable to identity fraud:

- the number of known fraud schemes committed against your organisation;

- the number and status of fraud allegations your organisation has received that required investigation;

- the number of fraud investigations resolved;

- the number of employees who have/have not agreed to and signed your code of conduct;

- the number of employees who have/have not completed ethics training that you sponsor;

- the number of whistleblower allegations received via your hotline;

- the number of allegations made by other means;

- the number of messages supporting ethical behaviour that your executive team has delivered to employees;

- the number of vendors who have/have not agreed in writing to comply with your ethical behaviour requirements;

- your benchmarks with global fraud surveys, including the types of fraud experienced and average losses;

- the number of customers who have agreed in writing to comply with your ethical behaviour requirements;

- the number of fraud audits performed by internal auditors;

- the results of employee or other stakeholder surveys concerning the integrity or culture of your organisation; and

- the resources your organisation has used.

....

[33] **www.aicpa.org/download/news/2008/Managing_the_ Business_Risk_of_Fraud.pdf**

The measurement techniques you adopt will depend on organisation-specific factors, such as the controls you use, the fraud risks identified and the resources available. Specific measurement techniques include:

- the fraud recurrence rate;
- how quickly you implement remediation plans;
- how quickly you implement additional controls to prevent further fraud;
- your assessments of the likelihood that frauds perpetrated against other organisations in the same industry will occur in your organisation;
- comparisons of fraud cases with complaints, grievances, etc received via your hotline;
- comparisons of the number of fraud cases discovered with the number of fraud audits performed; and
- the ratio of problems revealed in background checks and the number of checks performed.

The *EOI Standard* includes other potential performance measures.

9.1.2 Across-government performance measures and monitoring

Government agencies (individually and at a sector level where appropriate) are encouraged to set targets and monitor their performance as part of achieving the government's goal of reducing the incidence and costs associated with identity crime.

The Department of Internal Affairs, as part of its responsibility for ensuring that "New Zealand's approach to identity is trusted and well led" will collect information periodically about the incidence and costs of identity fraud, while implementing the *Identity Assurance Framework.* However, it recognises that it will take time for agencies to phase in their processes for collecting this information.

Information will be consolidated to provide an all-of-government view, not reported by individual agency.

9.2 YOUR PERFORMANCE MEASUREMENT CHECKLIST

- ✓ Does your organisation have performance measures in place?
- ✓ Have your performance measures been developed alongside a risk assessment process?

The types of information that will be sought from agencies (for the 1 July to 30 June period)

MEASURE	HOW MEASURED?
Incidence of detected identity fraud (confirmed and suspected)	Number of cases of identity fraud detected. A breakdown of confirmed and suspected identity fraud cases, under categories such as system checks, staff checks/ internal controls, and anonymous tip-offs from the public.
Detected identity fraud as a percentage of total transactions	Number of cases where identity fraud is detected as a percentage of total transactions.
Number of prosecutions taken (where identity fraud was involved)	Number of prosecutions taken.
Percentage of cases where prosecution successful	Number of completed cases successfully prosecuted and sentences ordered.
Estimated losses associated with identity fraud	The direct losses for financial fraud as well as an estimation of indirect costs to your organisation. Examples include: • investigation costs – staff costs and overheads; • time lost; and • non-financial items stolen.
Estimated recovered costs	Costs recovered directly from fraudsters.

GLOSSARY OF TERMS

For the purposes of this Guide, the following definitions apply:

TERM	DEFINITION
Control[34]	A process, effected by the governing body of an organisation, senior management and other employees, to provide reasonable assurance that risks are managed and the organisation's objectives are achieved.
Deterrence[35]	Strategies undertaken by an organisation to discourage people from initiating fraudulent activity.
Deterrence controls	Controls that involve convincing potential fraudsters that fraud against an organisation is not worthwhile – and therefore eliminating a fraud attempt that might have otherwise happened.
External fraud[36]	Fraud committed by someone outside an organisation, e.g. a customer or third party provider.
Governance	In the widest sense, how any organisation, including a nation, is run. It includes all the processes, systems and controls that are used to safeguard and grow assets. Overall, governance involves systems and practices that promote enterprise and ensure accountability. This Guide is concerned specifically with the governance of identity fraud controls within organisations that face identity-related risks.
Identity crime[37]	A generic term to describe activities/offences in which a perpetrator uses a fabricated identity; a manipulated identity; or a stolen/assumed identity to facilitate the commission of a crime(s).[38]
Identity fraud[39]	The gaining of money, goods, services and other benefits or the avoidance of obligations through the use of a fabricated identity, a manipulated identity or a stolen/assumed identity. Identity fraud is most often a component of criminal activity.
Identity information	Personal details collected about an individual. For any given identity attribute, the government often has one agency that has the best capability for collecting, verifying, maintaining and asserting that attribute.

---

[34] Source: *Fraud Control in Australian Government Agency Better Practice Guide*

[35] Source: *Fraud Control in Australian Government Agency Better Practice Guide*

[36] Source: *Fraud Control in Australian Government Agency Better Practice Guide*

[37] Source: *Standardisation of Definitions of Identity Crime Terms: A Step Towards Consistency*

[38] Such as: identity fraud and relevant related offences, including the possession, distribution and manufacture of relevant items, devices etc; people smuggling and trafficking; drug trafficking; terrorism; and money laundering

[39] Source: *Standardisation of Definitions of Identity Crime Terms: A Step Towards Consistency*

Identity theft[40][41]	The theft or assumption of a pre-existing identity (or a significant part of one), with or without consent. The victim may be alive or dead. Identity theft happens in a multitude of ways, ranging from somebody using someone else's credit card details illegally to make purchases over the internet or telephone to somebody assuming someone else's entire identity to do things such as open bank accounts, take out loans, make tax returns and conduct other business illegally in their name.
Internal controls[42]	Any policies, procedures, techniques and mechanisms put in place to minimise process failures and help ensure that actions are taken to address risks.
Internal fraud[43]	Fraud committed by an employee directly against the organisation for which they work.
Investigation[44]	Searching collated evidence connecting or tending to connect a person (either a natural person or a body corporate) with conduct that infringes the law or the policies and standards set by the affected entity.
Prevention[45]	Strategies designed to proactively reduce or eliminate fraud committed against an organisation.
Prevention controls	Controls to stop attempted fraud from occurring or to secure the organisation and processes against internal and external fraud.
Risk appetite	The level of risk to which an organisation is willing to be exposed, when balanced with a level of convenience and efficiency for staff and customers.
Risk assessment[46]	The application of risk management principles and techniques in the assessment of the risk of identity fraud to an organisation.

[40]Source: *Standardisation of Definitions of Identity Crime Terms: A Step Towards Consistency*

[41]Source: **www.direct.gov.uk/en/CrimeJusticeAndTheLaw/ Typesofcrime/DG_174616**

[42]Source: *Evidence of Identity Standard:* **www.dia.govt.nz/ diawebsite.nsf/wpg_URL/Resource-material-Evidence-of-Identity-Standard-Index?OpenDocument**

[43]Source (modified): **Fraud Control in Australian Government Agency Better Practice Guide**

[44]Source (modified): *Fraud Control in Australian Government Agency Better Practice Guide*

[45]Source (modified): *Fraud Control in Australian Government Agency Better Practice Guide*

[46]Source (modified): *Fraud Control in Australian Government Agency Better Practice Guide*

EXTERNAL GUIDANCE REFERENCES

REFERENCE	WEBLINK
Anti-Spam – Department of Internal Affairs	www.dia.govt.nz/Services-Anti-Spam-Index
Australian/New Zealand Standard Risk Management (AS/NZS 4360:2004)	www.standards.govt.nz/default.htm
Baseline Personnel Security Standard (UK)	www.cabinetoffice.gov.uk/media/45160/hmg_bpss.pdf
Bell Gully's Practical Guide	www.bellgully.com/resources/pdfs/Anti-Money-laundering-Countering-Financing-of-Terrorism-Bill-Jul09.pdf
Code of Conduct – State Services Commission	www.ssc.govt.nz/display/document.asp?navid=296
Code of Banking Practice – New Zealand Bankers' Association	www.nzba.org.nz/banking-standards/code-of-banking-practice/
Crimestoppers	www.crimestoppers-nz.org/
Data matching – Office of the Privacy Commissioner	www.privacy.org.nz/data-matching-introduction/
Evidence of Identity Standard	www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Evidence-of-Identity-Standard-Index or https://psi.govt.nz/evidence/default.aspx
Fraud Act 2006 (UK)	www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060035_en.pdf
Fraud Control in Australian Government Agency Better Practice Guide	www.wbde.org/references/Reference_A-G's_FraudControlInAustralianAgencies20.pdf
Fraud and Misconduct Survey 2010 (KPMG)	www.kpmg.com/NZ/en/IssuesAndInsights/ArticlesPublications/Pages/Fraud-Survey-2010.aspx
Good Practice Guide on Pre-Employment Screening (UK)	www.cpni.gov.uk/Docs/Pre-employmentscreening.pdf
Guiding Principles for the Use of Biometric Technologies for Government Agencies	www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Guiding-Principles-for-the-Use-of-Biometric-Technologies-Index?OpenDocument or https://psi.govt.nz/biometrics/default.aspx

Identity Assurance Framework	www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Publications-Identity-Assurance-Framework?OpenDocument
International Organization for Standardization Risk Management – Principles and Guidance (ISO 31000:2009)	www.iso.org/iso/catalogue_detail.htm?csnumber=43170
Managing the Business Risk of Fraud: A Practical Guide	http://fvs.aicpa.org/NR/rdonlyres/98BD10EC-CC12-4D14-848D-E5BDB181F4EE/0/managing_business_risk_fraud.pdf
Managing the Risk of Fraud – A Guide for Managers (UK)	www.hm-treasury.gov.uk/d/managing_the_risk_fraud_guide_for_managers.pdf
National Identity Fraud Awareness Week	www.stopidtheft.com.au/
New Zealand E-Government Interoperability Framework (e-GIF)	www.e.govt.nz/standards/authentication
New Zealand Crown Law Prosecution Guidelines	www.crownlaw.govt.nz/uploads/prosecution_guidelines.pdf
Privacy Awareness – Office of the Privacy Commissioner	http://privacy.org.nz/privacy-awareness-week/
Risk Management Guidelines (SAA/SNZ HB 231:2004)	www.standards.govt.nz/default.htm
Scamwatch – The Ministry of Consumer Affairs	www.consumeraffairs.govt.nz/scams/about-scamwatch
Standardisation of Definitions of Identity Crime Terms: A Step Towards Consistency	www.acpr.gov.au
Statement of Intent 2010-2013 – Department of Internal Affairs	www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Corporate-Publications-Statement-of-Intent-2010-13?OpenDocument

Tackling External Fraud, National Office Audit (UK)	www.nao.org.uk/guidance__good_practice/acquisitions-1/fraud_and_corruption.aspx
The National Compliance Qualifications Project	www.learningstate.govt.nz/upload/downloadable_files/Learning_State_Compliance_Project.pdf
Understanding Internal Controls: A Reference Guide for Managing University Business Practice	www.ucop.edu/ctlacct/under-ic.pdf

The following external references are not included in this Guide but may also provide some assistance

REFERENCE	WEBLINK
Fraud Prevention Scorecard in Managing the Business Risk of Fraud: A Practical Guide	www.acfe.com/documents/managing-business-risk.pdf
Governance and Fraud Control within Selected Adult Education Agencies	www.audit.vic.gov.au/reports__publications/reports_by_year/2009/20090603_fraud.aspx
How to Prevent Identity Crime – New Zealand Police	www.police.govt.nz/safety/home-identity-crime.html