Government of **Western Australia**
Department of **Commerce**
Consumer Protection

Mandatory CPD 2016

Real Estate Agents and Sales Representatives

Distance Learning Participant Manual

Case Study: Residential Focus

- **Cybercrime and identity fraud**
- **Changes to foreign investment legislation in Australia**

Government of **Western Australia**
Department of **Commerce**
Consumer Protection

IMPORTANT

This workbook and the accompanying presentation have been prepared for educational purposes only, as part of the **Department of Commerce Compulsory Professional Development Program**.

It is not, and should not be construed as, legal advice.

Any person in doubt as to their legal rights and obligations should seek the advice of a suitably qualified and competent legal practitioner.

Published by:	Department of Commerce
Developed by:	WCPT
Reviewed by:	TBA
First Published:	TBA
Version Number:	v1.0

Contents

Introduction

The purpose of this case study is to train residential licensees and sales representatives in identifying risk within their agencies. We will explore two contemporary risk areas:

1. The occurrence of cyber-crime and identity fraud; and,
2. Changes that have recently been proposed by the Foreign Investment Review Board relating to foreign investment in real estate in Australia.

The case studies have been built using a blend of real estate industry examples and risk management trends. However, attendees must realise that risk management is an inherently unstable area of business. It is critical that attendees take the information contained within the case studies as an introduction to the subject matter, and seek to extend their awareness of the issues raised.

Instructions

1. Complete this mandatory distance learning pack by reading this book and answering the questions as you go. These questions will help you test your understanding and knowledge. **This book is yours to keep!**
2. When you have finished the reading and writing in this book, you are required to **complete the 14 question Evaluation Exercise and return it for marking**.

Did you know…

Even though the case studies created in this document are current and represent legitimate threats to agency security, the risk landscape is constantly changing. Cyber-crime in particular is **constantly evolving.** What does this mean? Each of us must continue to educate themselves, keep our security practices up to date and maintain an awareness of evolving threats.

Case Study: Cyber Crime and Identity Fraud

Let's start with a story.

Radical Real Estate Co is a high performing Real Estate company experiencing strong growth in Perth's metro area. Radical employs 45 people across four office locations. In six months' time, Radical's CEO plans to launch franchise opportunities for Radical Real Estate Co, targeting two offices every six months over the next three years.

Radical Real Estate Co believes their point of difference is their commitment to pursuing excellence in technology and innovation. Radical has invested heavily in IT infrastructure.

Clients are so impressed with the service Radical Real Estate Co offers. They love the way Radical can target their property interests so specifically and appreciate the opportunity to deal with Radical Real Estate Co via email, phone, Skype or text message.

Radical Real Estate Co is on cloud nine. Until disaster strikes.

First, the sales administrator's computer becomes the target of a ransomware attack. When he returns from lunch, he finds his computer locked and a demand for $500 displayed on the screen. Apparently the system has been encrypted, and without the payment of $500, it will remain that way.

Then, the north coast office rings to report malware has been found on three computers in their property management department. Radical Real Estate Co has no idea of the degree to which their systems have been compromised – all they know is that personal information relating to every property, owner and tenant is stored on these machines.

Finally, the disaster that might just topple them – an owner of a property on Tree Street managed by Radical Real Estate Co calls to ask why he had been randomly sent a copy of a signed O&A document in spite of the fact that he has had zero communication regarding listing or selling the property.

Group Discussion

1. Summarise the problems Radical Real Estate Co is facing.

Here's a thought

Think about the immediate issues of crime and fraud, as well as impending customer service and reputation issues.

2. Who has been potentially impacted by the events that have unfolded at Radical Real Estate Co?

Here's a thought

There could be an impact to staff, customers, contractors – even Radical's own business partners and providers.

3. Does the uptake of new technology unavoidably expose agencies to new risks?

Here's a thought

When we say no to technology, we say no to opportunity. So we need to manage the risk of technology, not run from it.

Introduction to Risk

Businesses of every size are exposed to risk every day. Let's refresh the concepts of Risk, Threat and Risk Management.

What is risk?

> Risk is defined by the International Organisation for Standardisation (ISO) as:
>
> **The effect of uncertainty on objectives.**
>
> Effect: a deviation from the expected.
>
> Uncertainty: the state of deficiency of information related to an event, its likelihood and its consequence.
>
> Objectives: in a business context, objectives could be related to financial success, health and safety or the environment.
>
> *Adapted from ISO Guide 73:2009 (en) Risk management – Vocabulary – Guides for use in standards*

In other words, risk is what we didn't see coming.

Although the definition of risk is clear at a conceptual level, it can be difficult to articulate exactly how risk can impact ourselves, our staff, our businesses and our clients.

A simple way to make risk tangible is as follows:

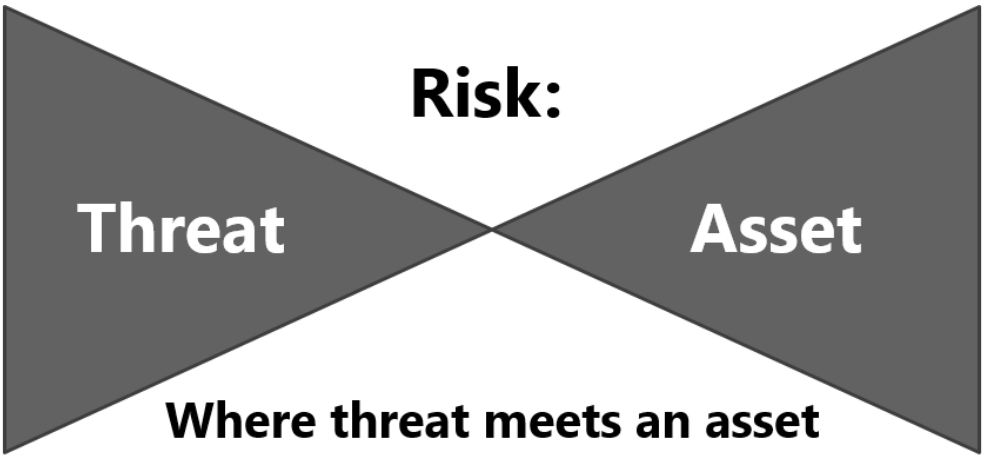


Figure 1: Risk Explained

A **threat** can be understood as either a mode of threat (such as a cyber-attack, a legislative oversight, or an environmental disaster), or a threat actor (an individual or group with an intent to cause harm). Threat modes are measured by likelihood and consequence, and threat actors are measured by intent and capability.

An **asset** doesn't need to be physical: it may be your staff, reputation, intellectual property, your business premises or IT infrastructure – or the properties owned by your clients.

Questions

4. Where does risk come from in a business?

Did you know…

There is a 'known unknown' nature to risk. We know that changing technology, crime and complex processes give rise to risk, but we do not always know when, where, or how.

5. How do we separate risk from threat?

Here's a thought…

Threats cannot be stopped – but we can introduce measures to reduce risk.

6. Who is responsible for identifying and managing risk in a real estate context?

Here's a thought…

Should every member of an office team be responsible for managing and implementing risk management strategies? And can we really protect against everything?

Risk Management

Risk management is about acknowledging that risk exists and finding a way to work around it. Effective risk management will minimise the impact of risk on a business – in fact, high performing business leaders are often able to create a competitive advantage by proactively and effectively managing risk.

What is Risk Management?

Risk Management is defined by the International Organisation for Standardisation (ISO) as:

The coordinated activities to direct and control an organisation with regard to risk.

This coordination would likely be achieved through the use of a risk management policy and plan.

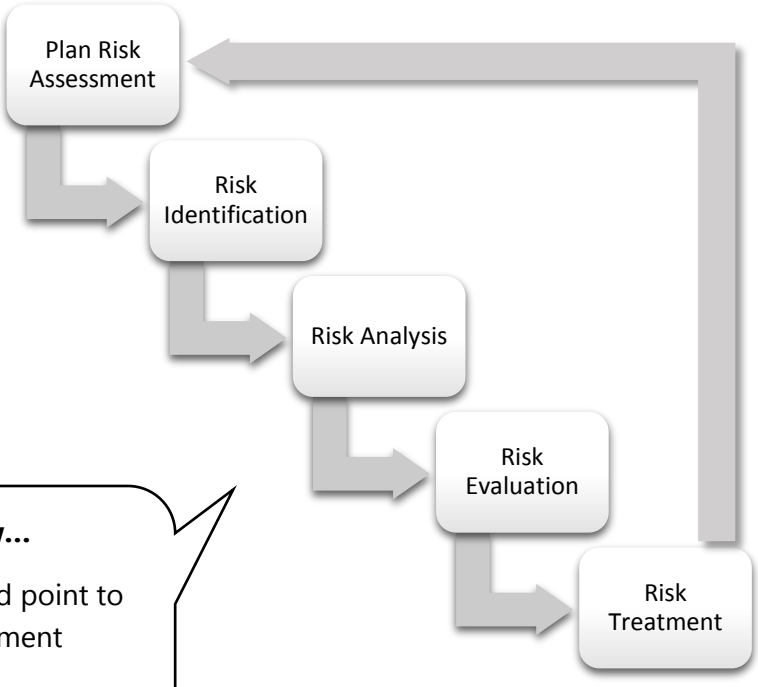
Risk Management Policy: a statement of the overall intentions and direction of an organisation with regards to risk management.

Risk Management Plan: a scheme specifying the approach and resources to be applied in the management of risk. This will include procedures and practices, accountability and responsibility, and timing of activities.

Adapted from ISO Guide 73:2009 (en) Risk management – Vocabulary – Guides for use in standards

In other words, familiarising ourselves with the unknown and making sure we are ready for it.

The Risk Assessment Process



Did you know…

There is no end point to the risk assessment process – it's a continuous cycle.

Figure 2: The Risk Assessment Process

An explanation of this process is included below:

Plan Risk Assessment	- A business will first plan to conduct a formal risk assessment - It may occur annually or twice annually, or even more often - Assessment owners are identified: who will conduct the assessment and who oversees the process?
Risk Identification	- Involves the identification of risk source, risk event, risk cause and risk consequence - Involves a thorough understanding of the threat landscape and organisational assets - The necessary information may be gathered by consulting historical data, experts and staff
Risk Analysis	- This is a formal process to determine the level of risk. - All identified risks are compared. - The analysis involves understanding the likelihood of something happening (or the exposure of the organisation to the risk), and the consequence should the risk be realised (monetary or otherwise).
Risk Evaluation	- This process ascribes a value to the risk that allows all risks identified to be ranked in order of impact and therefore importance. - A matrix is used to display the risks, which is achieved by defining ranges for consequence and likelihood. - This process will also consider an organisation's risk appetite – the amount of risk they feel comfortable with.
Risk Treatment	- This step involves a process to modify the risk. It may include avoiding certain activities, changing policies or processes, removing the risk source or taking steps to lower the impact or consequence of the risk. - Organisations will aim to mitigate or eliminate risks that produce wholly negative consequences.

Figure 3: The Risk Assessment Process in Detail

The process described above is then repeated at scheduled intervals, as organisations assess how their treatments have managed the risks previously identified, and determine whether there are new risks to be added to the list.

Case Study: More Detail

Radical Real Estate Co does some research to get to the bottom of the incidents that impacted their business:

Malware

- The malicious software in the north coast office had been identified when the antivirus software that runs on the system had been reactivated. Apparently, a staff member had disabled the antivirus software prior to a software update.
- The malware appeared to gain access to the computer when an employee clicked on some advertising on a webpage, while doing a spot of online shopping over a lunch break. The malware executed when the link was clicked, and was silently downloaded in the background. The malware was able to make its way onto other networked computers within the department.

Ransomware

- The ransomware was activated on the computer when a link was clicked within a dodgy email. The ransomware managed to encrypt the computer using the same technology that encryption programs use to protect information – but in this case, it was to restrict access until payment was made.
- Radical Real Estate Co contacted the police, who were unable to provide assistance. Although a backup had been made, it was over 6 months old. In the end, Radical's licensee decided he had no option but to pay the fee to regain access to their client information.

Social Engineering

- Radical Real Estate Co's licensee was stumped as to how an offer and acceptance for the Tree Street property could get all this way without an issue being raised. The under offer sticker was even already on the sign!
- Turns out, a fraudster had rung the office to update the email address details for the owner. Once complete, the bad guy had then requested the property be put up for sale – the owner instructed the property was to be sold for at least $600,000 and wanted a sale as quickly as possible. Low and behold, an offer for $602,000 was received on the first weekend the property was marketed! The fraudster dealt quickly and seamlessly with Radical Real Estate Co via a series of emails and telephone calls. The only thing that saved them was a seemingly redundant process step that had been around forever: post a copy of the O&A to a mailing address on file.

Threat Mode: Cyber-Attacks for Data Breach

Cyber-attacks that seek to obtain data for nefarious (dodgy) use come in many forms: malware and ransomware are two methods of attack.

Malware

Malware, or malicious software, is software that is designed to do damage to computer software.

Malware can take many forms and can be used to achieve many outcomes for a prospective hacker.

> Research by Verizon suggests 5 malware attacks occur globally every second.

Ransomware

Ransomware is a type of malware that locks data and demands that the owner of the data make a payment to have the data unlocked. The payment amounts demanded can vary, but generally ransomware hacks are sent out in significant quantities and the payment amount is low to convince a user it may just be easier to make the payment ($500, for example).

Entities looking to prosper and profit via a malicious software attack do not discriminate based on industry or profession: every computer is a target, and generally, the system's user inadvertently grants access to the hacker or program.

> Verizon research has found an average of 23% of phishing recipients open the email messages: 11% click on the attachments.

Social Engineering

A significant proportion of malicious cyber-attacks are achieved using some version of social engineering: that is, tricking a human to grant access to an illegitimate entity.

Phishing emails that trick people into providing sensitive information are a common tactic. Research by Verizon in 2015 has found an average of 23% of phishing recipients open the email message and a further 11% click on the attachments or links.

A further study has indicated that over 50% of phishing email opening occurs within an hour of the suspect emails landing in an inbox.

Threat Mode: Identity Theft

Identity theft is a type of fraud that involves using someone else's personal identification details to gain access to money or other benefits.

Social engineering is again one of the most common ways to accomplish a theft of identity. Although we often consider email to be the primary danger zone for phishing activity, the phone is in fact the primary method for 'phishing' for personal details. In 2015, the ACCC suggested over 40% of phishing occurred via phone, whereas email represented 24% of efforts and SMS only 3%.

According to the ACCC, over 40% of phishing scams occur over the phone.

Here's a thought…

If we are 'tricked' by a fraudster, does that excuse us from our responsibilities under the Code of Conduct?

Code of Conduct

9. Standard of service

> An agent must exercise due skill, care and diligence.

10. Duties as to details of the transaction

> (4) Without limiting the generality of subsection (1), an agent must, as soon as practicable after receiving instructions to act for a person in arranging a disposal, by way of sale, exchange or otherwise, of real estate and before a contract for that disposal is executed, make all reasonable efforts to verify —
>
> > (a) the identity of each person who claims to be, or to act for, a person who is to dispose of all or any of the real estate; and
> >
> > (b) each person's authority to dispose of the real estate, or to act for the person disposing of it, as the case requires.

Question

7. Discuss the relevance of the Code of Conduct in those instances where staff have been tricked into abandoning the usual security practices.

Managing Cyber and Identity Risk

The Risk Management process will assist real estate businesses in managing and mitigating the risks associated with cyber-attacks and identity theft. Given the propensity for such an attack to impact business, it is likely that Radical Real Estate Co's licensee is now looking for a simple and rigid framework to guide his risk management efforts.

The PPRR Framework

New technology and evolving threat modes mean cyber and identity theft risks are changing all the time. This means our risk management approaches must continually evolve to keep up. This diagram provides a clear plan for organisations in managing risk. First, organisations must take ongoing and evolving steps to Prepare and Prevent. Then, in the case where a risk is realised, the Respond and Recover activities allow for a systematic and careful reaction.

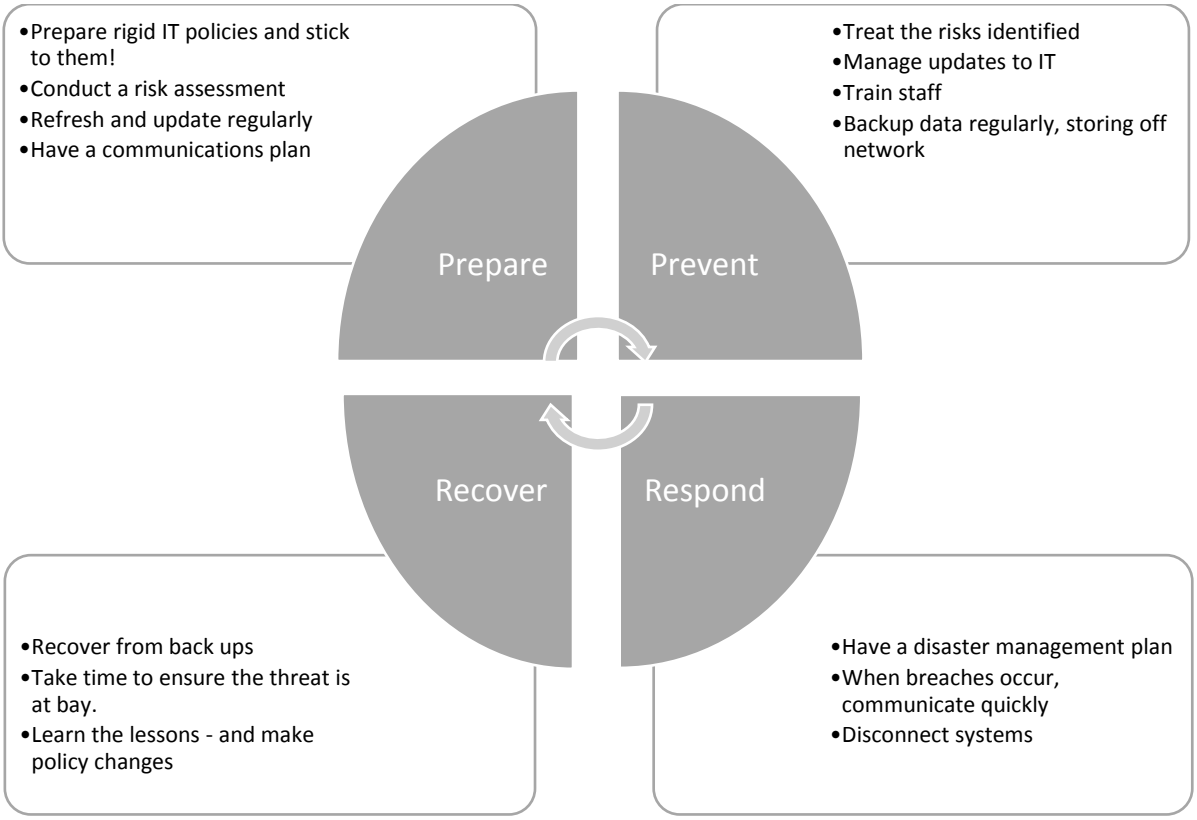


Figure 4: PPRR

The PPRR framework does not replace a risk assessment process – it adds an extra level of analysis and planning for those risks deemed to be of particular significance or impact to a business.

Using PPRR in our Cyber and Identity Theft Case

We will now use the PPRR model to assess how Radical Real Estate Co could have improved their management of the issues identified.

Activity

8. Let's work backwards – assume the fraudulent behaviour was successful, but that Radical Real Estate Co had comprehensive Respond and Recover actions in place. Under each heading, detail what these actions would have been, and what the impact on the business and its assets would have been.

Respond	Recover
Here's some thoughts to get you started: *Radical Real Estate Co had thought about the worst case scenario and had a disaster recovery plan in place. This meant they were able to;* - … - … - …	*Radical Real Estate Co were able to action the planning they had completed as part of ongoing risk management activities. This meant they were able to;* - … - … - … **Here's a thought…** Think about disaster recovery and reputation preservation.
Impact:	

9. Next – let's consider the actions that may have significantly reduced the likelihood of the risks being realised – or, significantly reduced the impact. What actions should Radical Real Estate Co have taken to Prepare and Prevent? Note the actions and summarise the impact on the business and its assets.

Prepare	Prevent
Here's some thoughts to get you started: *Radical Real Estate Co had completed a comprehensive risk assessment, which had allowed them to think about the types of cyber threats that might impact their operations. This meant they were able to;* - … - … - …	*Radical's risk assessment allowed them to implement preventative measures to counter the threat of cyber crime. These measures included:* - … - … - … **Here's a thought…** This exercise is all about trying to familiarise yourself with the unknown.
Impact:	

Summary

A significant number of cyber-attacks are enabled by a human. Awareness and education are therefore critical to managing cyber and identity-based fraud within a real estate business. Below are some key messages to communicate to teams and some tips to Prevent and Prepare within your business.

1. **Work is for work**: computers connected to your office network should be used for work purposes. Personal use of a work computer exposes the system to unnecessary risk.
2. **Understand your privacy responsibilities**: The Privacy Act sets responsibilities for businesses, including how information is handled and what must occur in the event of a breach.
3. **Social media is a great tool for fraudsters**: an abundance of personal identifying detail is shared on social media, which could result in an accidental exposure to someone with malicious intent. To avoid this, delineate between those social media applications that will be used in a professional capacity versus those that are for personal use, and do not link them. Also be aware that contact details can be obtained via agency websites.
4. **Manage your mail**: use email filters to halt emails before they arrive in a user's inbox – limit the opportunity for users to accidently click on the link by removing access to possibly nasty emails altogether.
5. **Consider a whitelist**: for systems that store critical data (such as financial details or client identification details), consider a whitelisting approach. The opposite of blacklisting, whitelisting dictates the programs that are *allowed* to run on a system. If a piece of malware is not on the list, it will be unable to run – also great for trust accounting purposes.
6. **Build a culture of communication**: talk about trends and developments in cyber fraud. Seek feedback from staff and ensure they do not feel scared to raise a risk or a suspicious email or call. Have procedures to cross-check and question requests.
7. **Use sensible IT security measures**: keep passwords strong and up to date, use a firewall to counter remote intrusion and update your software as soon as updates become available and use an antivirus program that screens emails and attachments. In the event of a security breach, unplug and turn off your computer immediately.
8. **Assess and reassess your risks**: A risk management process is not a static activity to be conducted one a year. Undertake regular assessments to ensure you have a pulse on how risk within your agency has evolved.

A watering-hole is a compromised legitimate website, frequented by a target user. In 2014, the Australian Cyber Security Agency handled more than 8100 watering-hole incidents.

Case Study Two: Foreign Investment in Australia

Radical Real Estate has implemented some robust risk management practices around cyber-crime and identify theft. Let's check in with them.

Radical Real Estate Co has experienced some hair-raising times over the past six months. Nevertheless, the CEO has had support of the office licensees and staff in implementing a rigorous risk assessment and management program. With risks identified and mitigated, Radical has been able to achieve their growth target: there are now 7 Radical offices.

Matthew is a rising star in the Radical group. He runs the newly opened Perth City office, and has grown the team steadily over the last six months. As licensee, Matthew believes his point of difference is in his team's commitment to serving international purchasers looking to enter the Australian real estate market. Matthew knows that foreign investment is great for the Australian economy, and that growing economies in South East Asia are looking for safe and stable financial environments in which to invest.

The Radical team has kicked of a significant marketing campaign in Malaysia, Indonesia and Singapore to attract investors to work with them. They have employed staff with diverse language skills and cultural awareness to assist them in building productive relationships. Matthew makes sure his team know to advise their clients of Australian legislation, including FIRB responsibilities.

One sunny Perth afternoon, Matthew takes a call from an irate gentleman named Thomas. Thomas has purchased more than 6 properties with Radical, including an existing dwelling from Radical five months ago as a temporary resident. He has now been told by the Australian government that he is not legally entitled to own the property. The purchaser is furious, and accuses Matthew and Radical of shirking the rules and trying to make a quick buck.

Question

10. Does Matthew have any responsibility in this situation?

Here's a thought…

It is critical that Matthew act in accordance with ***all*** legislation governing the activities of a real estate representative or agent. In this case, Matthew *may* be in breach of his responsibilities under the Foreign Acquisitions and Takeovers Act 1975 as well as the Criminal Code Act 1995.

“It is the Government's policy that foreign investment in Residential Real Estate should increase Australia's housing stock.

That is, the policy seeks to channel foreign investment in the housing sector into activity that directly increases the supply of new housing (such as new developments of house and land, home units and townhouses) and brings benefits to the local building industry and its suppliers.”

Foreign Investment Review Board

Why is foreign investment important to the Australian economy?

In 2013-14 financial year, foreign investment in Australian residential property was valued at over $34 billion dollars. This high level of foreign investment drives employment, productivity growth, and innovation.

Foreign investment is regulated by the Foreign Investment Review Board and the *Foreign Acquisitions and Takeovers Act 1975*. There are strict rules in place to ensure foreign investment is conducted in a lawful way. In 2015, the federal government announced a tightening of these laws. The changes include:

- All residential real estate approval functions were transferred to the Australian Taxation Office (ATO). The ATO can use its data-matching systems to identify possible breaches, which will allow the federal government to pursue foreign investors who break the rules.

- An increase in active monitoring of breaches to foreign investment rules, commencing with divestment orders (forcing the sale of a home) and then civil pecuniary penalties and infringement notices for less serious breaches from December 2015.

- Stricter penalties to make it easier to track foreign investors who breach the rules. Criminal penalties were increased to $135,000 or three years imprisonment for individuals and to $675,000 for companies; persons who assist those who break the rules will also be a target for penalties.

Changes to Foreign Investment Legislation

The Commonwealth government introduced changes to the *FATA* in order to strengthen the integrity of the foreign investment framework. The following table outlines the penalties for breaches of rules which apply to residential real estate:

Breach of current rule	Proposed new penalties
Foreign person acquires new property without approval *(approval would normally have been granted)* **Temporary resident acquires established property without approval** *(approval would normally have been granted)*	**Increased Criminal Penalty** Maximum criminal penalty of Individual — 750 penalty units ($135,000) or 3 years imprisonment (Bill suggests "or both"). Company — 3,750 penalty units ($675,000). **Civil Penalty** Maximum civil penalty is the greater of the following: 10 per cent of purchase price in addition to the relevant application fee; or 10 per cent of market value of the property in addition to the relevant application fee. **Tier 1 Infringement notice — Voluntary complied by coming forward** Individual — 12 penalty units ($2,160) plus the relevant application fee. Company — 60 penalty units ($10,800) plus the relevant application fee. **Tier 2 Infringement notice — Identified through compliance activities** Individual — 60 penalty units ($10,800) plus the relevant application fee. Company — 300 penalty units ($54,000) plus the relevant application fee. Either an infringement notice or civil penalty would be sought but not both.
Non-resident acquires established property or temporary resident acquires more than one established property	**Increased Criminal Penalty** Maximum criminal penalty of Individual — 750 penalty units ($135,000) or 3 years imprisonment.

(not normally approved) **Temporary resident fails to sell established property when it ceases to be their principal residence** *(breach of conditional approval)* **Temporary resident rents out an established property** *(breach of conditional approval)* **Failure to begin construction within 24 months without seeking extension** *(breach of conditional approval of vacant land/redevelopment applications)*	Company — 3,750 penalty units ($675,000). **Civil Penalty** Maximum civil penalty is the greater of the following: the capital gain made on divestment of the property; 25 per cent of purchase price; or 25 per cent of market value of the property.
Developer fails to market apartments in Australia *(breach of advanced-off-the-plan certificate)*	**Criminal Penalty** Maximum criminal penalty of: Individual — 750 penalty units ($135,000) or 3 years imprisonment. Company — 3,750 penalty units ($675,000). **Civil Penalty** Maximum civil penalty of: Individual — 250 penalty units ($45,000) Company — 1,250 penalty units ($$225,000)
Property developer fails to comply with reporting conditions associated with approval *(breach of advanced-off-the-plan certificate)* **Foreign person fails to comply with reporting condition which requires them to notify of actual purchase and sale of established properties** *(a new rule)*	**Civil penalty** Maximum civil penalty of: Individual — 250 penalty units ($45,000) Company — 1,250 penalty units ($225,000) **Tier 1 Infringement notice — Voluntary complied by coming forward** Individual — 12 penalty units ($2,160) plus the relevant application fee. Company — 60 penalty units ($10,800) plus the relevant application fee. **Tier 2 Infringement notice — Identified through compliance activities** Individual — 60 penalty units ($10,800) plus the relevant application fee. Company — 300 penalty units ($54,000) plus the relevant application fee.

	Either an infringement notice or civil penalty would be sought but not both.
Person assists foreign investor to breach rules	**Civil penalty** Maximum civil penalty, the same as the primary breach, of: Individual — 250 penalty units ($45,000) Company — 1,250 penalty units ($225,000) **Criminal Penalty** Knowingly assisting another person to commit a criminal offence is an offence under Section 11.2 of the Criminal Code (maximum penalty is the same as the primary offence).

Foreign investment threshold changes and application fees: Real estate investments

Type of investor	Type of acquisition	Previous threshold	New threshold	Application Fee from 1 December 20151
All investors (unless exempt)	Residential properties valued at $1 million or less	$0	$0	$5,000
	Residential properties valued at greater than $1 million	$0	$0	$10,000 (then $10,000 incremental fee increase per additional $1 million in property value)
	Advanced off-the-plan certificates	$0	$0	$25,000 upfront, with a six monthly reconciliation of properties sold to foreign persons based on rates above
	Annual Programs	$0	$0	$25,000 (or $100,000 where proposed investment is greater than $1 billion

Source: http://jbh.ministers.treasury.gov.au/media-release/034-2015/

Case Study: More Detail

Of particular importance to licensees and sales representatives is the increased focus on penalising those individuals who assist foreign buyers in acquiring real estate assets illegally. With this in mind, let's work out what happened with Thomas and Matthew.

Thomas has a long history with Radical, having purchased more than 6 properties off the plan, and lets Matthew know that he will soon be relocating to Perth for an extended period. Thomas has been granted a temporary resident visa and will be heading to Perth in the next few weeks – Thomas is aware he can purchase an established dwelling as a temporary resident.

Over a period of weeks travelling to and from Perth, Thomas successfully purchases his dream home in Applecross – alas, his relocation is delayed! He asks Matthew if Radical would mind renting the home out to a tenant on a short term basis and managing the property for him during this period. Matthew is happy to connect Thomas to the property management department. Before long, Thomas is contacted by the Australian government and told that as a foreign citizen, he was not entitled to own the existing property. Thomas threatens Matthew with a civil law case, claiming Radical had not fulfilled their obligations.

Questions

11. What should Matthew have done to ensure he was meeting his obligations under foreign investment legislation?

Here's a thought…

Matthew would be in breach of foreign investment legislation if he were deemed to be a person assisting a foreign investor to breach rules. It should be further noted that, even if a licensee/sales representative does not commit an offence under the Act, they may still be liable to a client for breach of contract, negligence or misrepresentation under the *Australian Consumer Law* if they fail to advise foreign investors of the requirements of the Act.

12. Discuss the relevant sections of the Code of Conduct to this situation.

Here's a thought…

Sections: 7. Duty to behave fairly; 9. Standard of Service; and, 10. Duty as to details of the transaction are relevant.

13. How could Radical have used Risk Management processes to avoid this scenario?

14. Make some suggestions as to how Matthew and Radical could update their Prepare, Prevent, Respond and Recover processes to tackle the threat of legislative change.

Here's a thought…

We can use risk management to ensure we keep a watchful eye on legislative change.

FAQs Relating to Foreign Investment

Q: I obtained approval to buy a new dwelling as a temporary resident. My visa will soon expire. Do I need to sell my house before the visa expires or can I retain the property and rent it out when I am overseas?

A: As you have bought a new property, you are not required to sell the property and can rent it if you wish.

Q: ***I am a temporary resident and bought a second-hand property in Australia to live in. I plan to go overseas for six months and wish to rent the property out during this period. Is this allowed?***

A: No. Second-hand properties acquired by temporary residents cannot be rented out for any period of time while the person is still a temporary resident.

Q: I obtained approval to buy a second-hand dwelling while on a 457 visa but am now planning to return to my home country permanently. I understand that I am required to sell the property but are there guidelines on the time frame on when the dwelling must be sold? For example, do I have to commence selling it before I leave or can I commence selling it after I have left the country?

A: You must sell the property within three months of leaving. If you do not think you will sell the property within this time you must contact us immediately at: firbenquiries@treasury.gov.au.

Q: I have just been granted a temporary resident visa and intend to move to Australia within a few months. Am I eligible to buy an established (second hand) dwelling?

No. You must be living in in Australia to be able to seek approval to buy a second-hand property (as you would have to live in it).

Q:. *I live overseas. Can I purchase an established (second-hand) dwelling with the intention of demolishing it and building a new house?*

Yes with approval. Foreign non-residents need to seek approval to buy established *(second-hand)* dwellings for redevelopment and must meet the specific requirements for redevelopments.

Source: http://www.firb.gov.au/content/faq.asp

Sources

Australian Cyber Security Centre 2015, *ACSC Threat Report 2015*. Available from: https://acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf

Australian Signals Directorate 2015, *Application Whitelisting Explained*. Available from: http://www.asd.gov.au/publications/protect/application_whitelisting.htm

Foreign Investment Review Board 2014, *FIRB Annual Report 2013-14*. Available from: http://www.firb.gov.au/content/Publications/AnnualReports/2013-2014/_downloads/FIRB-AR-2013-14.pdf

Foreign Investment Review Board 2015, *Frequently Asked Questions*. Available from: http://www.firb.gov.au/content/faq.asp

Scam Watch 2015, *Phishing*. Available from: https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/phishing

The Treasury 2015, *Government strengthens the foreign investment framework*. Available from: http://jbh.ministers.treasury.gov.au/media-release/034-2015/

Verizon 2015, *Verizon Data Breach Investigations Report 2015*. Available from: http://www.verizonenterprise.com/au/DBIR/2015/

Other Useful Sources

Commerce website: www.commerce.wa.gov.au

WAScamNet website: www.scamnet.gov.au

Australian Cybercrime Online Reporting Network: www.acorn.gov.au

Stay Smart Online Alert Service: www.communications.gov.au/what-we-do/internet/stay-smart-online

Note

The Department of Commerce has produced a Guidance Note entitled *Code of Conduct for agents and sales representatives: Client identification verification and real estate fraud prevention*. Attendees may find this Guidance Note helpful in understanding the application of the Code of Conduct to instances of fraud or identity theft. The Guidance Note can be accessed at the following address:

http://www.commerce.wa.gov.au/sites/default/files/atoms/files/guidancenotecodeofconductagentsandsalesrep.pdf

(UPDATED) AUGUST 2012

Application whitelisting explained

1. Application whitelisting is one of the top four strategies in DSD's list of *Strategies to Mitigate Targeted Cyber Intrusions*. This document provides high-level guidance on what application whitelisting is, what it isn't, and how Information Technology Security Advisers can apply it effectively in a Windows-based environment.

Why implement application whitelisting?

2. Application whitelisting is designed to protect against unauthorised and malicious programs executing on a computer. It aims to ensure that only specifically selected programs and software libraries (DLLs) can be executed, while all others are prevented from executing.

3. While primarily implemented to prevent the execution and spread of malicious software (malware), it can also prevent the installation or use of unauthorised software.

4. Implementing application whitelisting across an entire organisation can be a daunting undertaking, however deployment to high-value and often targeted employees such as executive officers and their assistants can be a valuable first step.

What is application whitelisting?

5. Application whitelisting comprises the following technical steps:

   a. identifying specific executables and software libraries which should be permitted to execute on a given system;

   b. preventing any other executables and software libraries from functioning on that system;

   c. preventing users from being able to change which files can be executed.

6. An intermediate approach to application whitelisting is identifying entire directories from which users are allowed to execute programs, such as C:\Windows, C:\Program Files, or even C:\Program Files\Specific Application. This provides some measure of protection from applications executing outside the specified directories but it does not take into account a number of possible scenarios for compromise. This technique is better than not applying application whitelisting at all, but a more comprehensive approach should be considered at the earliest opportunity such as at the next Standard Operating Environment (SOE) refresh.

What application whitelisting is not

7. Providing a portal or other means of installation of only approved software is not application whitelisting. This does not prevent users from running software not listed on the portal, and will not prevent malware from executing and compromising a system.

8. Application whitelisting is not accomplished by simply preventing users from writing to locations such as C:\Windows or C:\Program Files. While this may prevent a user from installing some software, it does not prevent the execution of software residing in locations such as a user's desktop or temporary directories. These locations are commonly used by malware to infect a computer.

How to implement application whitelisting

9. Application whitelisting is commonly implemented using a combination of a software product for identifying and approving necessary executable and library files, and Access Control Lists preventing users from changing the approved files.

10. AppLocker is a set of group policy settings which are present in Microsoft Windows 7. Extending the capabilities of Software Restriction Policies in earlier versions of Windows, AppLocker allows multiple levels of enforcement as well as several methods of recognising whitelisted executables. Both AppLocker and Software Restriction Policies are free application whitelisting products that are provided with recent versions of Microsoft Windows.

11. There are a number of third party applications which provide similar functionality to AppLocker. Mention of these products does not imply endorsement by DSD. Among these are products such as Bit9 Parity Suite, CoreTrace Bouncer, Lumension Application Control and McAfee Application Control.

12. It is crucial that the software selected and configuration used covers both executables and software libraries. An omission of either of those could negate the security afforded by the whitelisting implementation.

13. Whitelisted executables should be positively identified via means other than merely by file name or directory location. This helps ensure malware cannot trivially masquerade as legitimate software.

Further information

14. The *Australian Government Information Security Manual* assists in the protection of official government information that is processed, stored or communicated by Australian Government systems: http://www.dsd.gov.au/infosec/ism/index.htm

15. DSD's *Strategies to Mitigate Targeted Cyber Intrusions* complements the advice in the ISM. The complete list of mitigation strategies can be found at:

http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

Contact details

Australian government customers with questions regarding this advice should contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or dsd.assist@defence.gov.au.

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.

Available from: http://www.asd.gov.au/publications/protect/application_whitelisting.htm