



Grant Thornton
An instinct for growth™

Institute of Internal Auditors Victorian Chapter Members' Meeting

Sorting the wheat from the chaff & how to keep the gems

May 2016

Katherine Shamai, Grant Thornton
Travis Merlo, Merlo Consulting



Preparation



What could IA encounter?

Controls weaknesses and gaps



Policy and procedures weaknesses and gaps



Non-compliance



Systemic failure





Using subject matter experts

- Use of specialist expertise as needed for specific reviews
- Fraud and corruption should be seen as specialist skill set
- Private investigations are a licenced and regulated industry





Why is this important?

Increasingly complex
and digitalised
environment

First on scene

Second highest method of detection
after tip-off
- ACFE, Report to the Nations 2016

International Standards for the Professional Practice of Internal Auditing – 1210.A2:

"Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud. "

International Standards for the Professional Practice of Internal Auditing – 1220.A1:

"Internal auditors must exercise due professional care by considering the...
probability of significant errors, fraud, or noncompliance... "



What is fraud?

Australia Standard AS 8001-2008

Dishonest activity causing actual or potential financial loss to any person or entity including theft of monies or other property by employees or persons external to the entity and where deception is used at the time, immediately before or immediately following the activity.

Crimes Act 1958

By deception dishonestly obtain property / financial advantage with the intention of permanently depriving the other it

Crimes Act 1958

- Obtaining property/financial advantage by deception
- False accounting
- Falsification of documents
- Conspiracy & conspiracy to defraud

Deception | Intent | Loss

Fraud triangle






In the field





How can IA come across fraud?

Type of review	Alert level	What might go wrong?
Standard internal audit review		Missed suspicious transactions / red flags
Data analytics		Missed suspicious transactions / red flags
Management initiated reviews		Reasons for management concerns not tested / scoped Fraud / misconduct not identified due to insufficient testing

Whistleblowers



Fraud red flags - financial

- PO / invoice number sequence and
- Invoice "doesn't look right", e.g. blurry or distorted logo
- Changes to bank account details between invoices
- Unusual purchases for a supplier
- Unusual purchases for the organisation
- High levels of purchases – by value and by volume
- Round amount invoices
- Splitting of PO / invoices to bypass delegations of authority
- Delivery address on invoices
- Unauthorised changes to master file data
- Unusually high expenses or purchases
- Inventory shortages
- Missing files
- Falsifying records
- Irregular/unexplained variances in financial information



Fraud red flags - behavioural

- ◆ "Control freaks"
- ◆ Bullying and intimidation
- ◆ Sense of entitlement
- ◆ Changes in an employee's lifestyle, spending habits or behaviour
- ◆ Employees living beyond their means
- ◆ Poorly written or poorly enforced internal controls, procedures, policies or security
- ◆ Failure to take action on results of internal/external audits or reviews
- ◆ Frequent complaints from customers
- ◆ Ignored employee comments concerning possible fraud
- ◆ Borrowing from co-workers
- ◆ Collectors or creditors appearing at work
- ◆ Excessive use of telephone to stall creditors
- ◆ Refusing to leave custody of records during the day
- ◆ Working excessive overtime
- ◆ Refusing to take annual leave
- ◆ Excessive rewriting under the guise of neatness

So what do you need?

- Use professional scepticism and judgment
- Think like a fraudster
- Be curious
- Pay attention to details
- Build trust and rapport
- Rely on your experience
- Think outside of the box
- Think on your feet and be flexible with your approach
- Trust your gut



Ask ***ONE MORE*** question!



Now what?

- Talk it through with a forensic specialist
- Secure hard copy evidence.. And keep it!
- Document verbal information
- Get consent if needed
- Engage professional investigators and forensic technology specialist early on

Collecting and storing



Institute of Internal Auditor Members Meeting

May 25



Preserving Digital Evidence
Travis Merlo



What is digital evidence?

Information and data of value to an investigation that is stored on, received or transmitted by an electronic device

Common Types of Digital Evidence

- Financial Transaction logs
- Emails
- Access Logs
- Pictures
- Documents (Spreadsheets, word documents, powerpoints, etc)

What devices should you be looking for?



Digital Evidence Continued..

When would we see digital evidence as being important?

- Before an incident
- During an incident
- After an incident

Don't limit yourself to one piece of evidence, keep your mind open!

**MINDS ARE LIKE
PARACHUTES**



What is a Digital Crime Scene?



Each digital device should be considered a crime scene

Would you enter a homicide crime scene?
Would you let your subject?

Strategies to secure evidence/crime scene:

- Recommend the subject leave the workplace/go on leave
- Restrict IT access – remote login/phone etc
- Where is the data physically located?
- Can it be physically secured?
- Is there backups of the data?
- Has the subject had access to the data?



Case Study

- Misconduct Investigation of a Government employee
- Allegations of collusion and conflict of interest relating to a large procurement
- Allegations based of emails recovered by another firm
- Subject had been on leave for 6 weeks and had no access to her emails
- Department failed to provide access to emails to investigator until 4 March 2016
- Subject allowed access to emails on.

<input type="checkbox"/>	Name
<input type="checkbox"/>	Fw: Meeting with supplier
<input type="checkbox"/>	Fw: Meeting with supplier
<input type="checkbox"/>	Fw: Scope for proposed but not to happen
<input type="checkbox"/>	Fw: Follow up on RFQ

An investigation is only as good as the information its based on.

Top-level Item Date

Tuesday, 1 March 2016 1:07:09 pm Aust...

Tuesday, 1 March 2016 1:07:58 pm Aust...

Notes Accessed	Friday, 4 March 2016 1:19:50 pm ...
Notes Added To File	Friday, 4 March 2016 1:19:50 pm ...
Notes Created	Tuesday, 1 March 2016 1:07:03 p...
Notes Modified	Friday, 4 March 2016 1:19:50 pm ...
Notes Revised	Tuesday, 1 March 2016 1:07:10 p...
OriginalModTime	Tuesday, 1 March 2016 1:07:10 p...
PostedDate	Tuesday, 1 March 2016 1:07:09 p...



What can I do?

- Remember – electronic evidence is volatile, and can be easily altered/deleted.
- Never 'Have a look' (remember – you wouldn't 'have a look' at a murder scene and potentially contaminate an entire investigation)
- Take notes, then take more notes, then some more. When you have finished taking those notes, take some more. Remember – if it is important enough to make a mental note about – WRITE IT DOWN.
- Why are notes important: Often court cases are years after an incident is uncovered.
- Contact a professional. Computer forensics, or *Cyber Investigations* is a specialised field. Contact someone who is an expert in the field.
- Realise your limitations – its ok not be an expert in every field
- If you have access to, or collect digital devices or digital evidence – create and maintain a chain of custody log.

- ✓ What did you eat for lunch, 3 years ago?
- ✓ Was it hot/cold?
- ✓ What was the weather like?
- ✓ Who was there, and what order did you see them in that day?
- ✓ What time did you eat?
- ✓ Did you use a napkin?

CRIME SCENE DO NOT ENTER





What is a chain of custody?

in legal contexts, refers to the chronological documentation or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence

Why is it important?

- Often court cases are years after an incident is uncovered
 - Is the integrity of your evidence intact?
 - Who has had access to your evidence? When? Why? How?
-
- Label your physical evidence (Date time location and who collected it, ID number)
 - Refer to the ID number in chain of custody record

Contact:

Travis Merlo
Director

Merlo Consulting
www.merloconsulting.com.au
m. +61 402008891
e. travis@merloconsulting.com.au



Contact

Katherine Shamai

Senior Manager – Financial Advisory

Grant Thornton Australia

W | www.grantthornton.com.au

L | au.linkedin.com/in/katherineshamai

T | +61 3 8663 6123

E | katherine.shamai@au.gt.com



Grant Thornton
An instinct for growth™

Institute of Internal Auditors Victorian Chapter Members' Meeting

Sorting the wheat from the chaff & how to keep the gems

May 2016

Katherine Shamai, Grant Thornton
Travis Merlo, Merlo Consulting

