Spencer's eGuides

Focussing on RISK

BUSINESS

FRAUD RISK

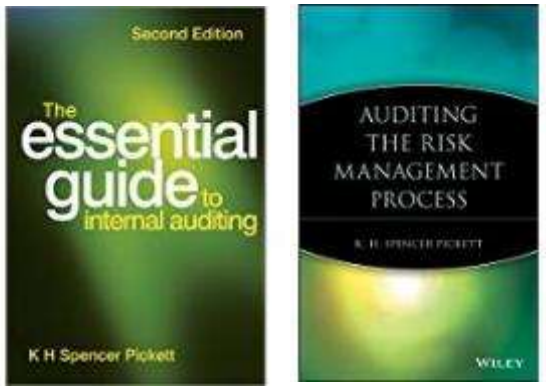
MANAGEMENT

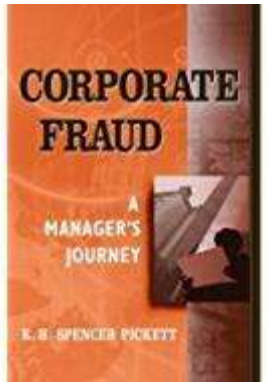
Please view landscape 'Full Screen Mode' using Adobe Acrobat Reader where possible.

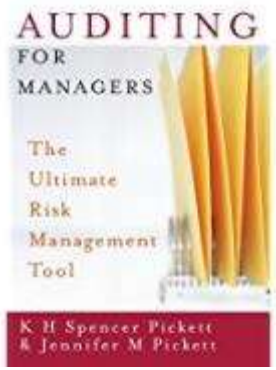
A Brief Message

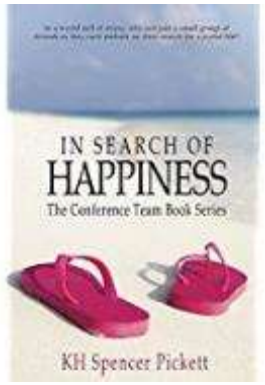
Welcome. My career has involved managing internal audit teams and audit training programs as well as writing about risk based auditing and related topics. More recently, I decided to prepare a series of simple guides focussing on Business Risk and how it can be best managed. I hope you enjoy your eGuides.

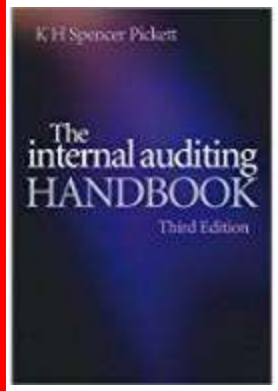
Spencer Pickett

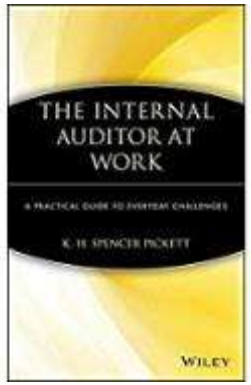


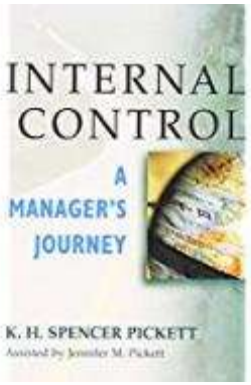


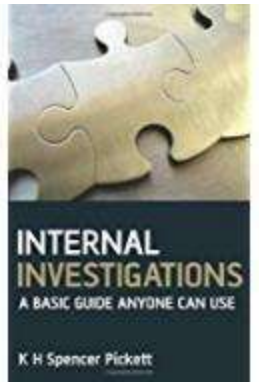


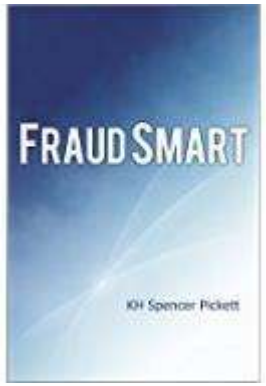


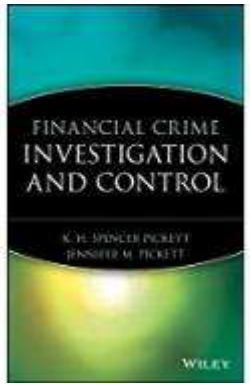


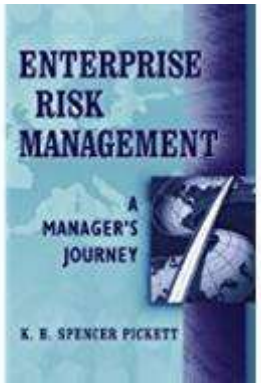


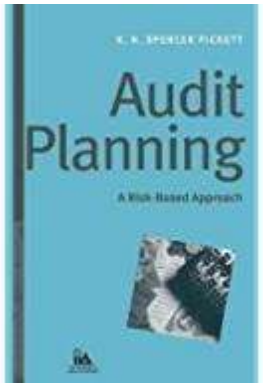












Spencer's eLearning Courses:

The Internal Audit Training Portal

Whistleblowing: When Should You Act?

Essential Fraud Awareness Training

Available at: Elearningmarketplace.co.uk

Your eGuide

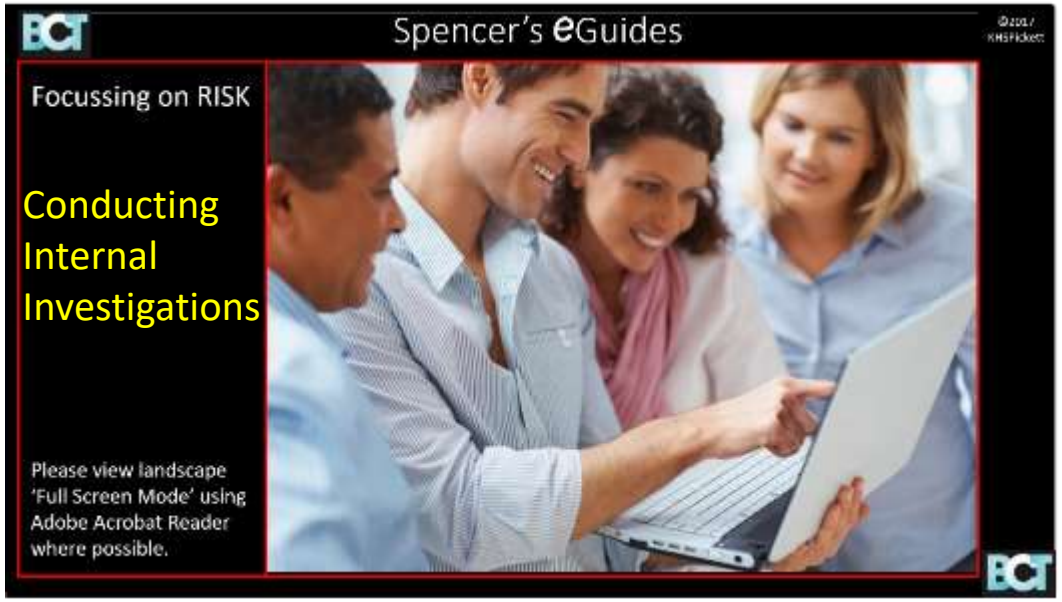
Your eGuides contain basic introductory material to help you deal with risk at work.

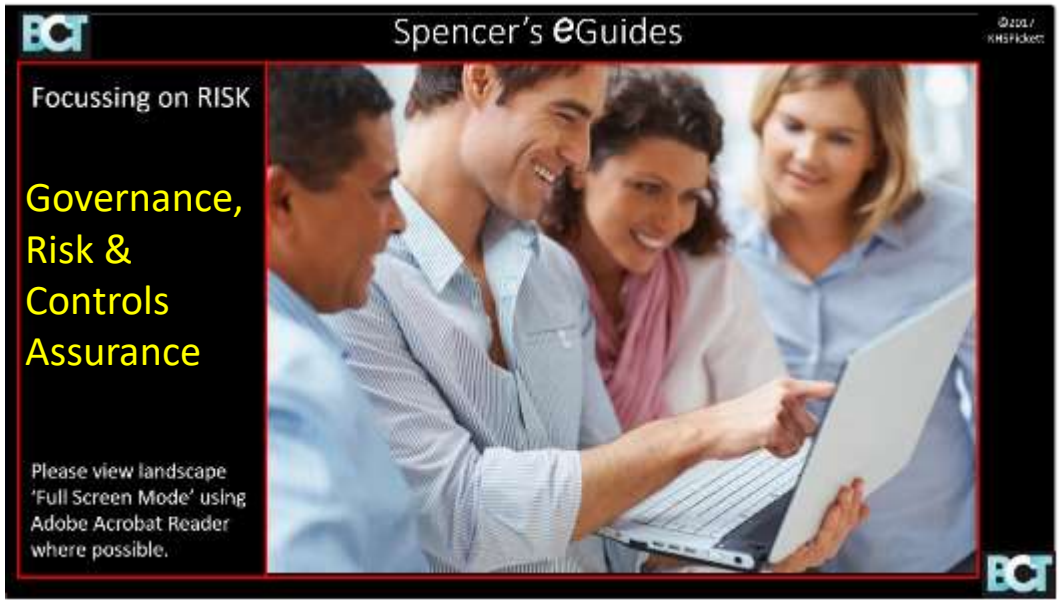
You should view this PDF using Adobe Acrobat Reader. For best results use landscape, 'Full Screen Mode'.

Your eGuide may only be viewed by persons authorised to do so under the purchasing terms and conditions.

Please note that you may not share or copy this PDF.

Your Four eGuides





List of Contents

Business Fraud Risk Management Template

Your Template

Business Fraud Risk Management

PART ONE:
YOUR TEMPLATE BRIEFING

For those who want an introductory briefing, Part One will take you swiftly through the Template on your right. After which you can simply stop if all you need is a short introduction to the topic.

PART TWO:
YOUR TUTORIAL

Your eGuide includes a Training Tutorial that provides a formal introduction to the topic based around your Template. There are also a few 'Read On If You Want More Details' pages which you can explore or just skim through.

Part One

Your Template: Introductory Briefing

Business Fraud Risk Management Template

Your Template Briefing

Business Fraud Risk Management

We'll be running through each part of your Business Fraud Risk Management Template.

Understanding The Risk of Fraud at Work

Deterring Fraud at Work

DEFINING ROLES

PARTY	ROLE

FRAUD RISK MANAGEMENT

RISK	PREVENT	DETECT

FRAUD RESPONSE

STAGE	ACTION

Red Flags

Prevent

Respond

Strengthen

CONDUCT

CONTROLS

Your Dynamic Role

True or False?

But first, let's get you to do some work. Have a look at each statement and tell me whether they are true or false.

Answers are on the next page.

Some Statements	True or False
Fraud can only happen when there is an actual loss involved.	
References are crucial when recruiting people as we need to know they are honest and above board.	
We may need to pay a backhander now and again to get things done in some foreign countries.	
Anti-fraud work should be left to the experts as it is their responsibility.	

Our Answers

Some Statements	Are they True or False?
Fraud can only happen when there is an actual loss involved.	Not really. You can be convicted of fraud if you attempt to defraud someone but are unsuccessful. Many frauds are stopped by solid controls that guard against unauthorised access which we will explore later.
References are crucial when recruiting people as we need to know they are honest and above board.	Agreed. Although, even where references have been verified, someone who has always been completely honest and trustworthy in the past may turn bad, and cause many problems at work.
We may need to pay a backhander now and again to get things done in some foreign countries.	This is true. But even if many companies pay up front cash to facilitate business abroad, you may still be committing an offence. And you can get yourself and your company in trouble if you are not careful.
Anti-fraud work should be left to the experts as it is their responsibility.	Partly correct. But the whole point of this Tutorial is that we are all part of the fight against fraud. So fasten your seat belt and we'll see how you can play your part.

How Did You Do?

Your Template Briefing

Business Fraud Risk Management

Do you know enough about fraud and its consequences?

This is your chance to find out.

We have developed a simple resource that represents the minimum you should know along with a few basic tips.

The idea is to get you thinking about your role and encourage you to do a bit more.

Let's get cracking on Part One and hopefully you can stay with us and get involved in Part Two.

Business Fraud Risk Management Template

Your Template Briefing

Business Fraud Risk Management

UNDERSTANDING FRAUD

Let's quickly run through each part of your Template. We start with the basics - that is the need to ensure the risk of fraud is properly understood. This is about defining fraud and being clear about what is out there that could undermine your ability to safeguard your business from deceit and any resulting losses.

Fraud is defined in 'Managing the Business Risk of Fraud: A Practical Guide', which was sponsored in 2008 by the Institute of Internal Auditors, the American Institute of Certified Public Accountants and the Association of Certified Fraud Examiners:
'Fraud is any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain.'

Let's Deal With:
UNDERSTANDING FRAUD

Your Template Briefing

Business Fraud Risk Management

DEFINING ROLES

The next part sets out the different roles and responsibilities for fraud control across the organization. Clarifying who does what helps determine exactly where you fit into the plan.

Once you can see why and how you can help, you can get involved. Our Tutorial suggests you need to show a clear Red Light to Fraud:

Let's Deal With:
DEFINING ROLES

Business Fraud Risk Management Template

Your Template Briefing

Business Fraud Risk Management

FRAUD RISK MANAGEMENT

A central part of the Template is the all-encompassing task of managing fraud. Your Tutorial suggests three main tasks are required to manage the risk of fraud:

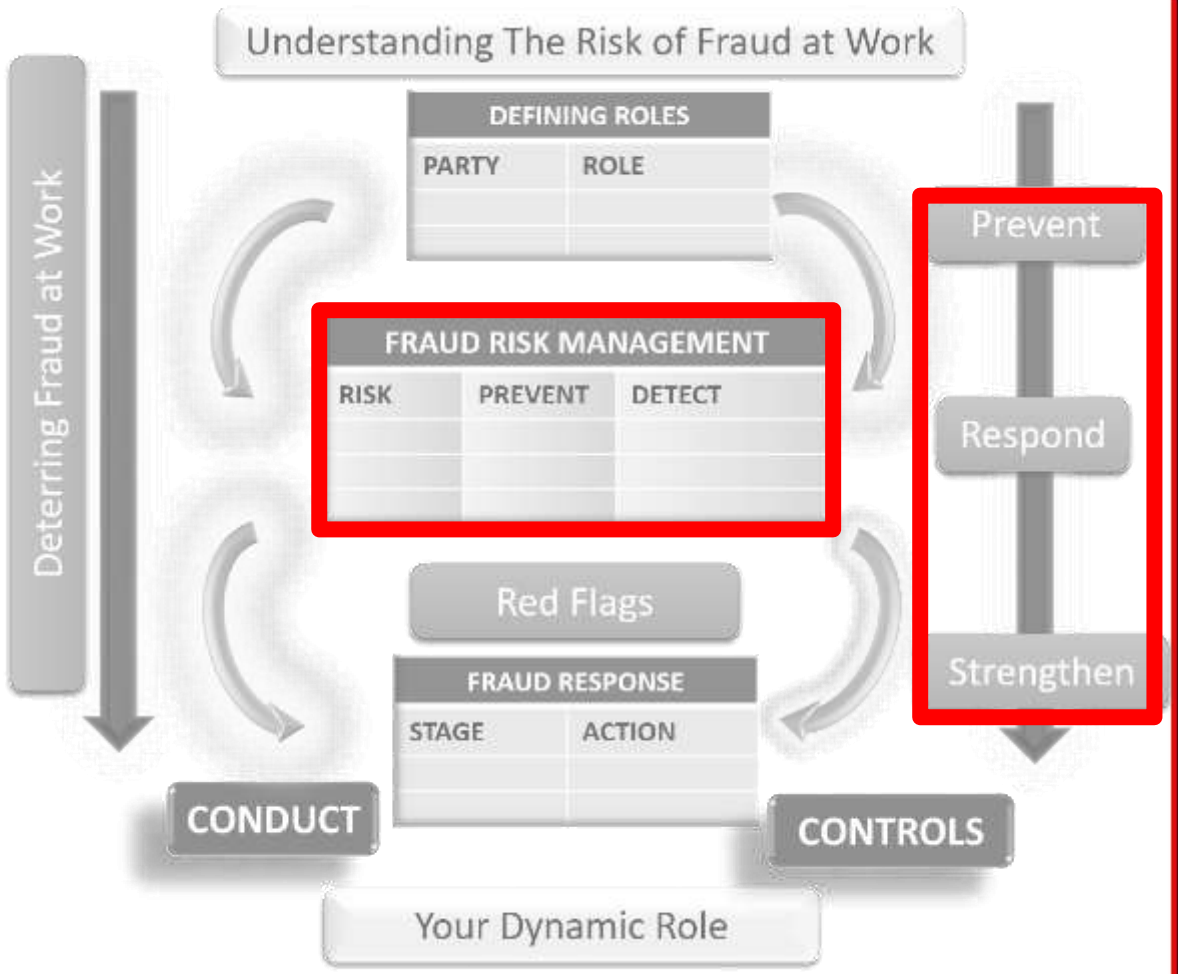
1. Establishing the risk of fraud.

2. Preventing the risk from materializing through sound controls.

3. And then detecting and responding to anything that gets through your defences.

PREVENT, RESPOND & STRENGTHEN

This feature reinforces the context for your Template. Preventing fraud, responding to it and making sure it never happens again.



Let's Deal With:
FRAUD RISK MANAGEMENT

Business Fraud Risk Management Template

Your Template Briefing

Business Fraud Risk Management

RED FLAGS

Your Template asks you to keep an eye out for fraud. This is about common sense but also being armed with an idea of some of the things that may suggest that all is not well. In some respects, the need to understand red flags and raise the alarm is not just a good idea, it is essential across the workforce.

Often, it is after a fraud has happened that people say, they thought something was wrong but didn't want to say anything.

Proactive fraud control is doing the opposite. Being alert to possible wrongdoing and speaking up. It is only by accepting your responsibility for fraud risk management that allows you to question oddities when for example, a colleague gets upset when anyone asks difficult questions about unusual decisions.

Let's Deal With:
RED FLAGS

DETERRING FRAUD

Everything in the Template is about deterring fraud. The sad fact is that fraud will happen if you don't ensure you have effective ways of stopping it. We argue that the Template is the least you should do in fighting fraud at work.

Deterring fraud is about being proactive. It is about running additional searches where you know that the process in place may allow unauthorised transactions.

It is about being engaged with the code of conduct and knowing when this is not being promoted properly in a way that encourages fair decision making.

Let's Deal With:
DETERRING FRAUD

FRAUD RESPONSE

Even with the best controls in place, fraud can still happen. Your Template includes some simple steps that you can take if and when you are faced with wrongdoing at work.

Your role does not extend to investigating fraud. Just being aware of the policies in place and what you need to do, and refrain from doing – in the event.

Appropriate fraud response is particularly important as the veracity of evidence can be challenged if a case comes in front of the criminal courts.

Let's Deal With:
FRAUD RESPONSE

Business Fraud Risk Management Template

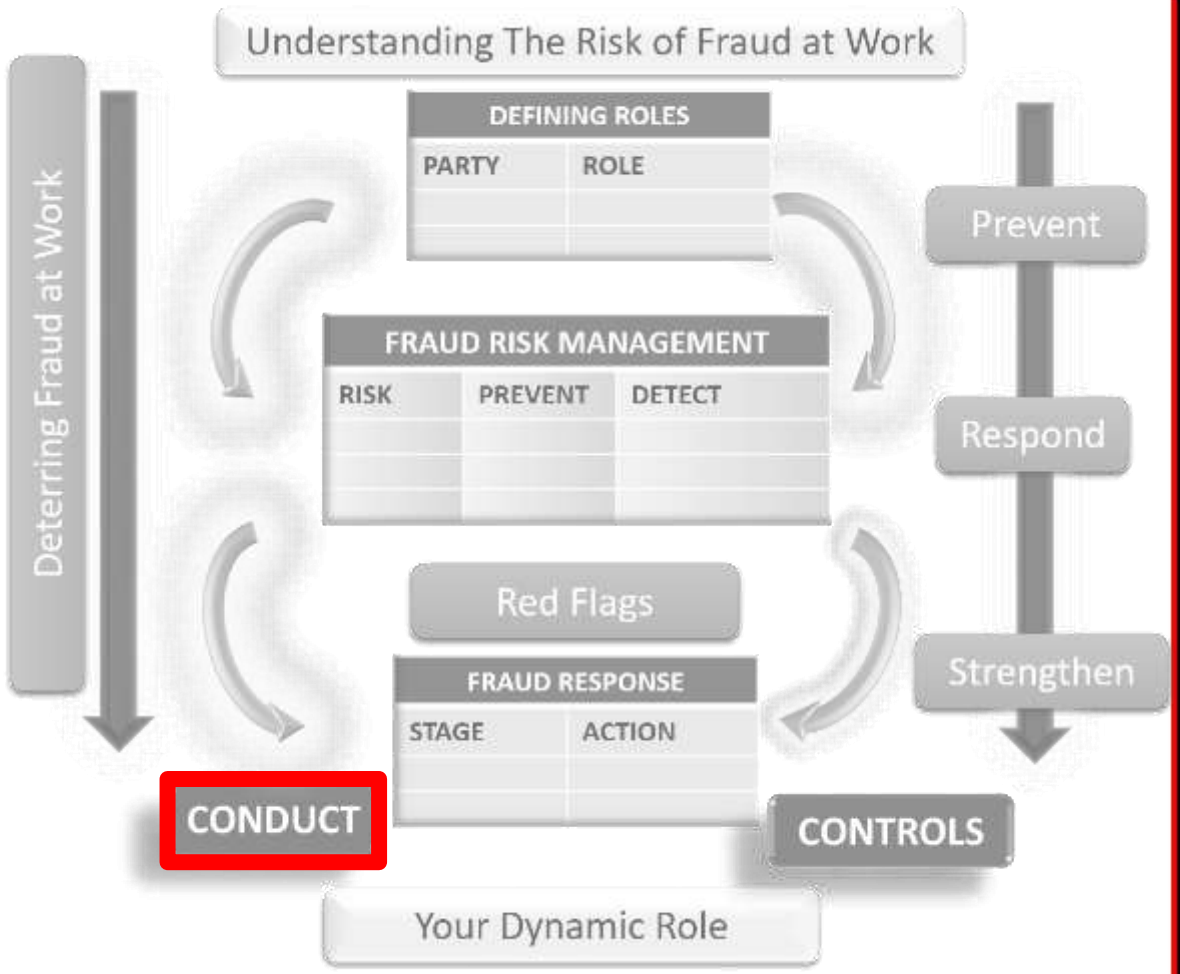
Your Template Briefing

Business Fraud Risk Management

CONDUCT

This feature is there to make sure you are able to deal with the way people behave at work. Conduct is about setting standards, ensuring they are met and dealing robustly with any shortfalls. Where fraud is involved, the usual position is to get rid of the culprit, recover any losses and activate the criminal justice system.

In the past, bad behaviour was often covered up and the perpetrator asked to quietly leave. A zero tolerance approach, or what we call our Red Stop Light model, involves seeking the full prosecution of anyone involved in fraud and corruption at work.



Let's Deal With:
CONDUCT OF STAFF

Business Fraud Risk Management Template

Your Template Briefing

Business Fraud Risk Management

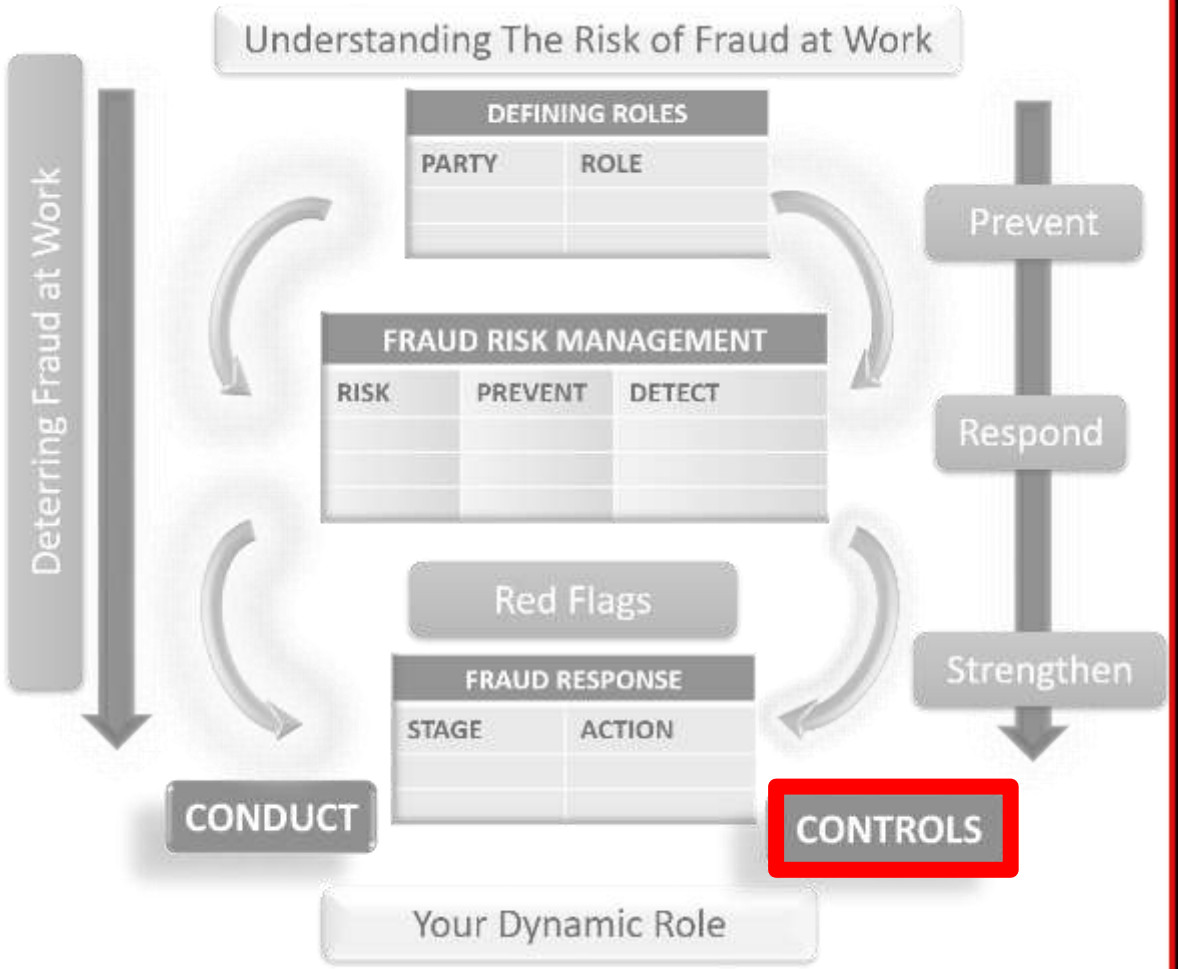
CONTROLS

Your Template has a go at listing some of the basic controls that should be part of your anti-fraud ammunition. The idea is to throw appropriate controls at the risk of fraud to give yourself the best chance of avoiding attack.

This is no easy task because it means admitting where controls are weak or are not being applied properly.

It also means you have not done enough in the past to ensure unauthorised access or inappropriate transactions are stopped from getting through your systems.

Good risk management is about being in charge of what happens at work and not allowing foreseeable risks to materialise. And this normally equates to sound controls.



Let's Deal With:
CONTROLS AT WORK

YOUR DYNAMIC ROLE

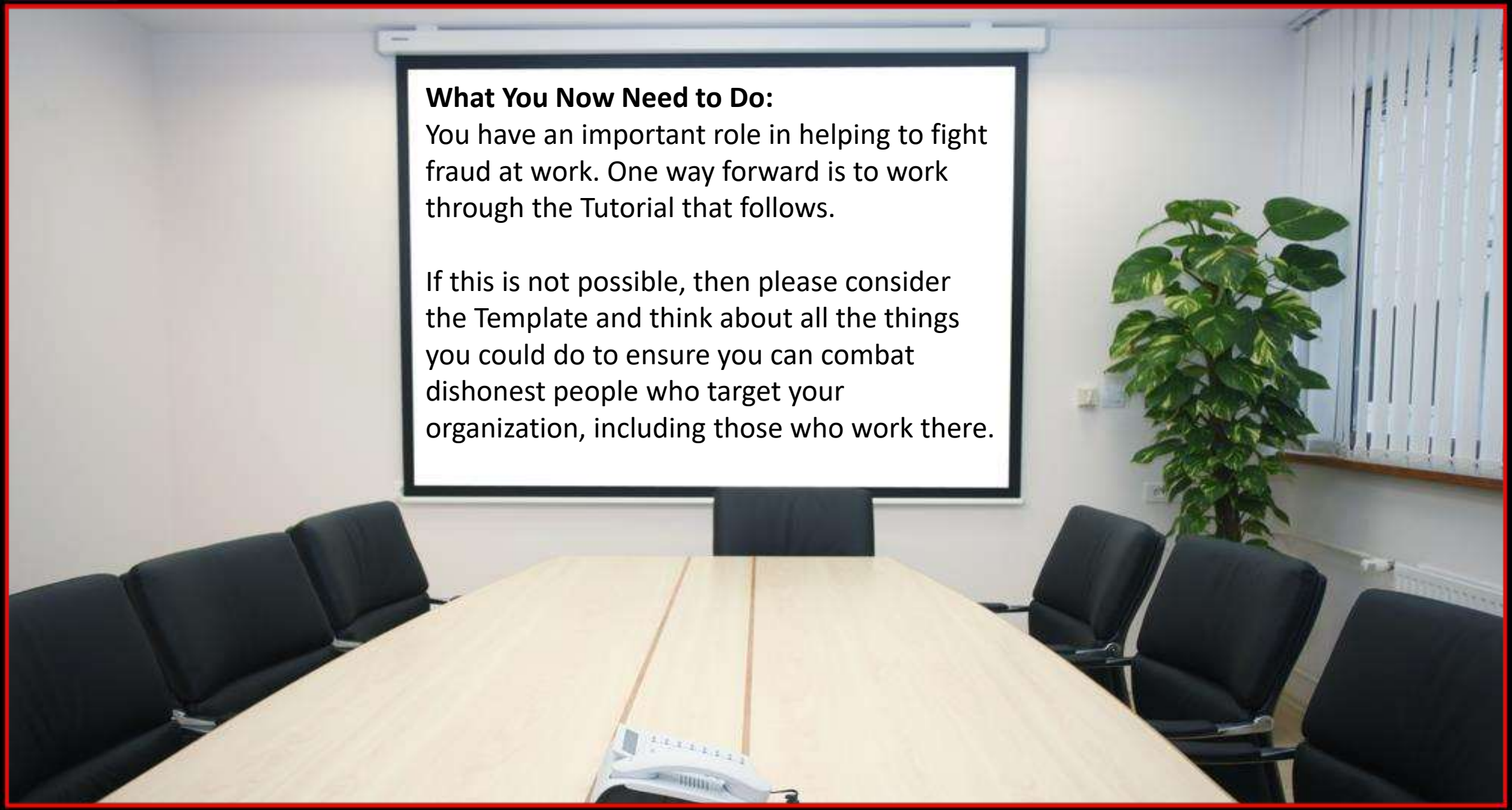
We close your Template with a few tips and techniques for engaging with your anti-fraud policy.

This means being dynamic in doing all you can, to be alert to the risk of fraud and mobilizing the efforts of your team wherever possible.

The idea is to send out a clear Red Light to fraud.

Let's Deal With:
YOUR DYNAMIC ROLE

Your Briefing Challenge



End of Part One

Okay, that's your intro done.

If you have had enough of your brief tour you can stop.

If you want more than just a glimpse into this topic then set aside an hour or so of your time, make yourself comfortable and start work on the Tutorial that follows.

End
of
Part One

Part Two

Your Tutorial

Training Aims

We have one simple aim for this Training Tutorial.

You will be tackling each part of a specially prepared Template that covers business fraud risk management.

We have included a few further information pages that drill down into the topic being viewed. You may choose to read these pages or simply skip them. You do not have to study these 'extra' pages to achieve the training aims.

A Question

There is no point being suspicious of everyone at work as most odd things have a completely harmless explanation.

Would you chose 1, 2 or 3 as the most appropriate response? We'll follow this up on the next page.

?

1. Agreed. It is best to leave the question of fraud to the experts.

2. Maybe. But getting involved and making accusations will always end badly for the accuser.

3. It's never a good idea to get into office gossip and jump the gun.

An Answer

Sorry, but this is a trick question as we believe all three options are inappropriate.

Another approach would be to say – if you have any concerns, then do something about it.

The next page will illustrate some of the things that fall under the 'office gossip'.

?

1 ✗ Agreed. It is best to leave the question of fraud to the experts.

2 ✗ Maybe. But getting involved and making accusations will always end badly for the accuser.

3 ✗ It's never a good idea to get into office gossip and jump the gun.

Check Out the Office Gossip

Introducing Your Tutorial

Business Fraud Risk Management

The Correct Answers

We'll return to the office gossip towards the end of your Tutorial

Your Tutorial

1. UNDERSTANDING FRAUD RISK

A Question

Fraud is any …… act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain.

Would you chose 1, 2 or 3 as the most appropriate response for the missing word? The correct answer is on the next page.

?

1. 'dishonourable'
2. 'intentional'
3. 'systematic'

An Answer

We need to use the word 'intentional' to reinforce the way fraud arises not by chance or neglect but by a clear intent to deceive.

1 ✗ 'dishonourable'

2 ✓ 'intentional'

3 ✗ 'systematic'

?

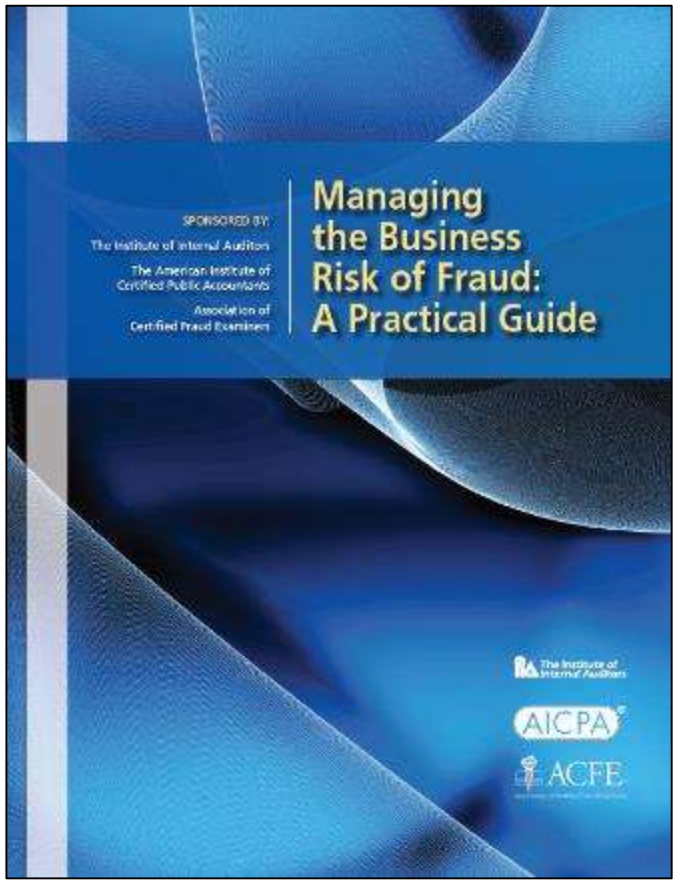
Your References

There are loads of guides and sources that deal with the topic of fraud and how best to deal with this worrying and growing risk. We don't want to overload you in this short eGuide, so we will refer mainly to two expert publications that have a global reach.

1. 'Managing the Business Risk of Fraud' sponsored by the Institute of Internal Auditors, The American Institute of Certified Public Accountants and the Association of Certified Fraud Examiners.

2. 'Report to the Nations' an annual report from the Association of Certified Fraud Examiners.

Let's have a look at the principles from Managing the Business Risk of Fraud.



Managing the Business Risk of Fraud contains five key principles:

Only through diligent and ongoing effort can an organization protect itself against significant acts of fraud. Here are 5 Key principles for proactively establishing an environment to effectively manage an organization's fraud risk.

Principle 1: As part of an organization's governance structure, a fraud risk management program should be in place, including a written policy (or policies) to convey the expectations of the board of directors and senior management regarding managing fraud risk.

Principle 2: Fraud risk exposure should be assessed periodically by the organization to identify specific potential schemes and events that the organization needs to mitigate.

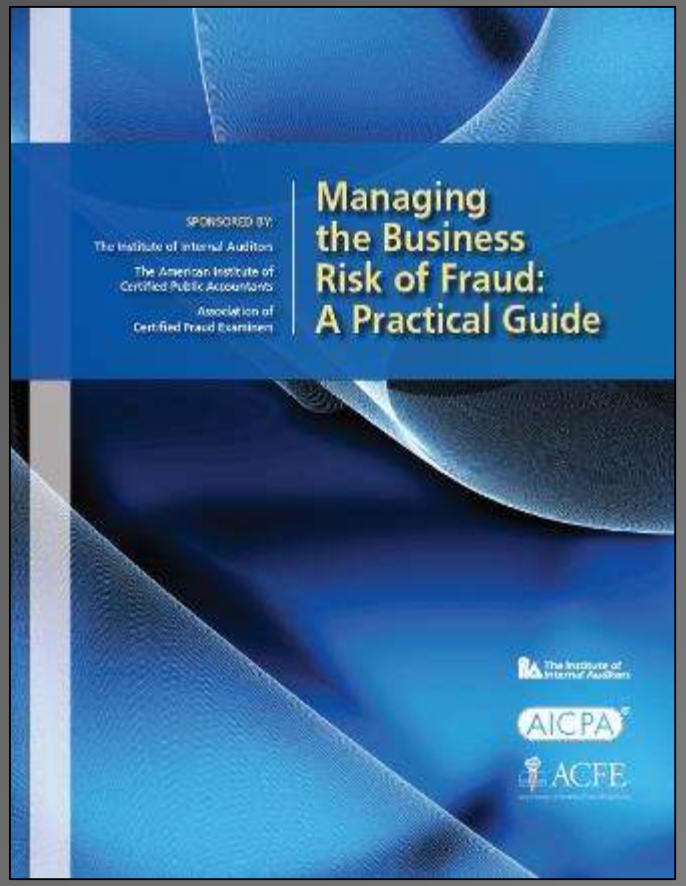
Principle 3: Prevention techniques to avoid potential key fraud risk events should be established, where feasible, to mitigate possible impacts on the organization.

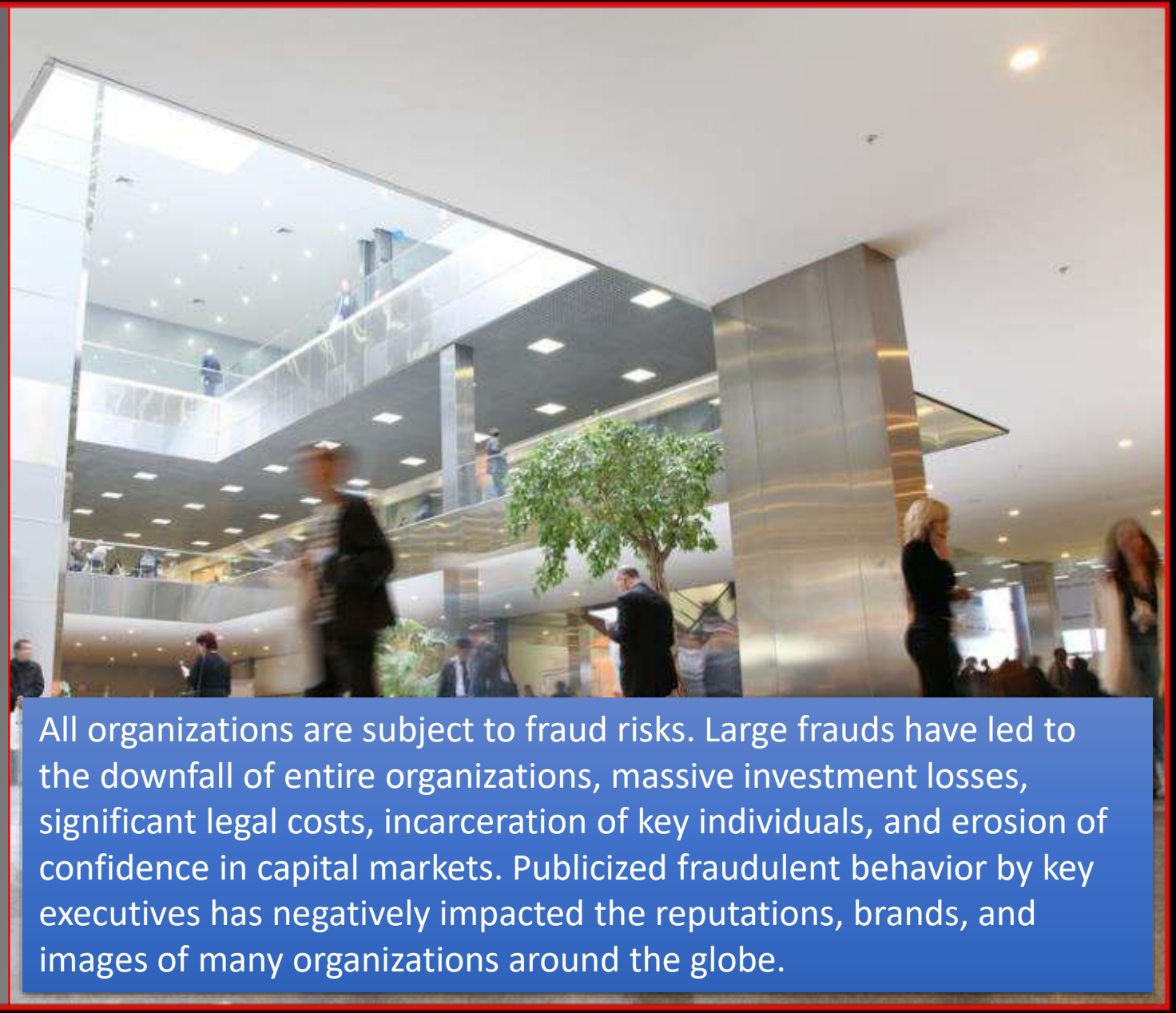
Principle 4: Detection techniques should be established to uncover fraud events when preventive measures fail or unmitigated risks are realized.

Principle 5: A reporting process should be in place to solicit input on potential fraud, and a coordinated approach to investigation and corrective action should be used to help ensure potential fraud is addressed appropriately and timely.

Managing the Business Risk of Fraud

A powerful quote for you.





All organizations are subject to fraud risks. Large frauds have led to the downfall of entire organizations, massive investment losses, significant legal costs, incarceration of key individuals, and erosion of confidence in capital markets. Publicized fraudulent behavior by key executives has negatively impacted the reputations, brands, and images of many organizations around the globe.

The Scale of the Problem

How big is the threat of fraud at work?

Some shocking figures from the Association of Certified Fraud Examiners in their Report to the Nations 2016.

'The CFEs who participated in our survey estimated that the typical organization loses 5% of revenues in a given year as a result of fraud. The total loss caused by the cases in our study exceeded $6.3 billion, with an average loss per case of $2.7 million.'

If you want to explore some legislation we have provided a brief account in the next few pages.

UK Legislation

The UK's Fraud Act 2006, which came into force in January 2007 created a new general offence of fraud with three ways of committing it:

- Fraud by false representation - where an individual dishonestly and knowingly makes a representation that is untrue or misleading.
- Fraud by wrongfully failing to disclose information - where an individual wrongfully and dishonestly fails to disclose information to another person when they have a legal duty to disclose it, or where the information is of a kind that they are trusted to disclose it, or they would be reasonably expected to disclose it.
- Fraud by abuse of position - where an individual who has been given a position in which they are expected to safeguard another person's financial interests, dishonestly and secretly abuses that position of trust without the other person's knowledge.

The act also created new offences:

1. Obtaining services dishonestly.
2. Possessing, making and supplying articles for use in frauds.
3. Fraudulently trading - applicable to non-cooperative traders.

The Serious Fraud Office investigates and prosecutes serious or complex fraud, bribery and corruption. The SFO works closely with many organizations including:

- The National Crime Agency.
- The City of London Police.
- UK Police Forces.
- HM Revenue and Customs.
- The Financial Conduct Authority.

US Legislation

In the United States, the 2002 Sarbanes-Oxley Act was an attempt to regain public trust in the wake of massive frauds such as Enron and WorldCom, that shook the investment community to its core. Section 404 asks for a periodic review of internal controls over financial reporting in an attempt to help combat fraudulent financial reporting. Sarbanes-Oxley also contains provisions that protect whistleblowers who report illegal or unethical behaviour. Meanwhile the American Institute of Certified Public Accountants (AICPA) has published Fraud Detection in their auditing standard, SAS No. 99, as part of the overall move to deter corporate fraud.

The U.S. Department of Justice enforces Federal laws. Federal investigative agencies with major consumer protection responsibilities, such as the Federal Bureau of Investigation, the Federal Trade Commission, the Securities and Exchange Commission and the Postal Inspection Service, refer numerous civil and criminal prosecutions to the Department. In pursuing these cases, they seek to protect consumers against dangerous and worthless products and unfair or fraudulent practices. It does so through the enforcement of consumer protection statutes, regulations, and orders. The Department has filed numerous actions in recent years against individuals and businesses committing fraud or violating laws and regulations that are intended to eliminate misrepresentations in the sales of goods and services.

Extracts from the FBI Financial Crimes Report to the Public, Fiscal Years 2010-2011, (October 1, 2009 - September 30, 2011):
The Federal Bureau of Investigation (FBI) investigates matters relating to fraud, theft, or embezzlement occurring within or against the national and international financial community. These crimes are characterized by deceit, concealment, or violation of trust and are not dependent upon the application or threat of physical force or violence. Such acts are committed by individuals and organizations to obtain personal or business advantage. The FBI focuses its financial crimes investigations on such criminal activities as corporate fraud, securities and commodities fraud, health care fraud, financial institution fraud, mortgage fraud, insurance fraud, mass marketing fraud, and money laundering. These are the identified priority crime problem areas of the Financial Crimes Section (FCS) of the FBI. The mission of the FCS is to oversee the investigation of financial fraud and to facilitate the forfeiture of assets from those engaging in federal crimes.

Why So Much Fraud?

The UK's National Fraud Authority no longer exists but they issued a report a few years ago that suggested there are three interlinked reasons why fraud has been on the increase for many years now.

A fraudster can sit on his or her computer, anywhere in the world and try to break into your business with little fear of being found out and prosecuted.

The solution is solid Cyber Security arrangements. We are focussing on employee fraud where someone close by is dishonest and has the ways and means of defrauding your business. Or just gaining a dishonest advantage.

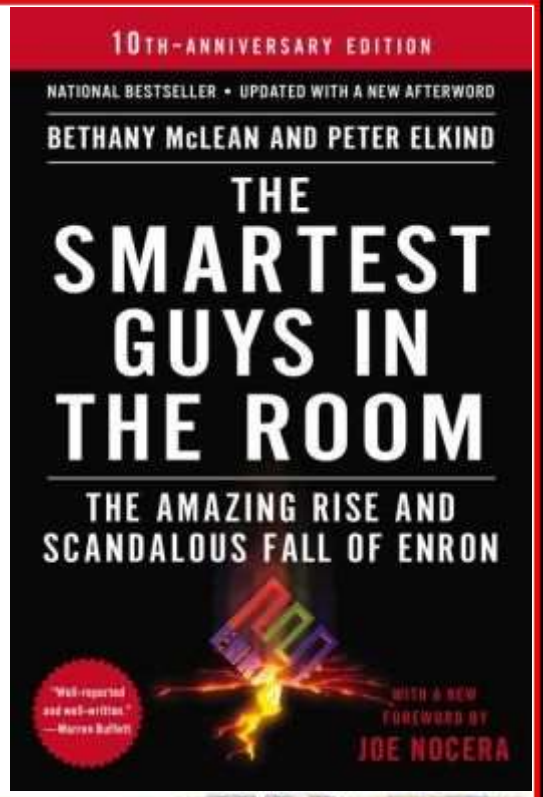
- Changes in business and organizational structures.
- Changes in the type of staff employed to service these new structures.
- Increased targeting of business by organized criminal networks.

On a wider front, an entire organization can get itself into a great deal of trouble when fraud is allowed to flourish.

The Enron collapse in the US led to huge losses for investors.

Moreover, this case reminds us that when company executives conspire to commit fraud and are found out, the consequences for everyone involved can be tremendous.

- Arthur Anderson, auditors, voluntarily surrendered its license to practice after being found guilty of criminal charges.
- Rick Causey, Chief Accounting Officer - pleaded guilty and testified against others. He was released in 2011.
- Clifford Baxter, Chief Strategy Officer - committed suicide in 2007.
- Andrew Fastow, CFO - cooperated with the prosecutors and served 6 years in jail.
- Jeff Skelling, CEO - sentenced to 24 years in jail
- Ken Lay, CEO and Chairman (before Skelling became CEO) - convicted of ten counts of fraud and later died of a heart attack.



Sherron Watkins, Vice President for Corp. Development (whistleblower) Is now a speaker on business ethics.

Three Famous Fraudsters

Do you remember the names of these three characters?

Three Famous Fraudsters

The key issue that arose was that most people had no idea that the people involved were fraudsters. In fact, Madoff expressed some surprise that he was not found out earlier.

Nick Leeson

Leeson was employed as a trader in Baring Futures (Singapore). He opened an unauthorized account, that he used to cover up his huge trading losses, which remained undiscovered until Barings collapsed in 1995.

Bernie Madoff

The Madoff fraud in the USA demonstrated quite clearly that people can be fooled into parting with their money. Madoff is now serving a 150 year sentence at a prison in North Carolina.

Allen Stanford

Stanford was jailed for the rest of his life for masterminding the largest fraudulent Ponzi scheme since the Madoff case.

A Few Famous Fraud Cases

- Ernest Saunders, the Chief Executive of Guinness, paid himself £3 million plus interest, and paid large sums to those who helped him rig shares in order to try and take over another drinks company, Distillers back in 1986. He rigged the shares to beat Argyll, the company in competition with him to try and take over Distillers. Ernest Saunders was not alone in the share-rigging as senior businessmen from outside Guinness were also involved. The key figures in this scandal were right at the very top of the organization so arguably, more junior members of staff working within finance may not even have been aware of what took place, let alone be able to question it.
- Robert Maxwell, the founder and Chief Executive of the Maxwell publishing empire, manipulated funds to give the impression that the company was financially liquid, in order to disguise the fact that he had perpetrated a huge fraud, which came to light in 1991. The official report into the Maxwell scandal revealed the problems with long-term relationships between external auditors and their client companies. Hailed as the biggest shake-up of auditing in 100 years, accountancy firms faced new guidelines designed to prevent conflicts of interests and a willingness to turn a blind eye to dubious behaviour to retain lucrative contracts.
- Anthony Williams, Deputy Director of Finance for the Metropolitan Police, was exposed as a fraudster. He stole £5 million over a period of eight years between 1986 and 1994 from a secret bank account, set up as part of a highly sensitive operation against terrorists. Anthony Williams was asked in the mid-1980s to set up this account. His signature was the only one required to authorize payments from the account, even though he had a co-signatory to the account. This enabled him to steal from the account to purchase homes in Spain, the South of England and a castle in Scotland, where he bought himself the title Laird of Tomintoul, and spent large amounts of money on property renovations. Williams was jailed for stealing £5 million. The Metropolitan Police described the Williams fraud as a 'one-off perpetrated by a clever, deceitful man who lived his life in compartments.'
- In 1996, it was revealed that Peter Young lost $600 million belonging to city bank Morgan Grenfell. Young, as head of Morgan Grenfell's European Growth Unit Trust in 1995, a fund worth £788 million, became interested in buying shares in a company called Solv-Ex. Solv-Ex's US directors claimed to be able to extract oil from sand cheaply. Peter Young spent approximately £400 million of his company's money on Solv-Ex. He set up 'shell' companies in Luxembourg to buy Solv-Ex shares illegally. In 1996, Solv-Ex was investigated by US federal agencies. By the time of his trial in 1998, Peter Young was declared mentally unfit. He attended court in women's clothing carrying a handbag.

Fraud Can Hurt

Fraud can also hurt people who take the wrong road. We would like to tell you a really sad story.

A promising young law student was the victim of a car rage incident and was attacked. She had to take sick leave and fell behind in her studies although she still attempted her exams.

She subsequently broke into the University at night and altered her exam results but was discovered. She could not face the shame of a court hearing and committed suicide at a nearby beach.

You need only type in 'fraud cases' if you want to read a vast array of illustrations from the internet. Many of them end up badly for all sides involved.

Dealing with Perceptions

It is quite possible to go through your working life and not realise that what you believe is happening is far from the truth.

Part of your new responsibilities is to reach out of your work cocoon and recognise when something is wrong. And what should be set procedures are not being followed.

It is a sad fact of life that people may not be all they seem as deceit is the corner stone of fraud.

We will be going through Red flags later on.

Why Worry?

Our Template suggests we should all be involved in the fight against fraud.

But taking on additional responsibilities is not always easy.

There are many reasons why people feel it is just too much extra work for something that may never happen.

The question is then, why should you bother?

Why Worry?

We dealt with the many reasons why we need not bother about fraud.

Here's a challenge for you.

Go back to the previous page and keep flicking between that and this page.

And for each of the reasons not to get involved in fighting fraud – look at the argument for doing the opposite. When you have done that then move on.

Slippery Slope

Fraud involves behaviour that may result in a criminal prosecution, while mistakes and waste are normally the result of poor judgement or substandard performance. This may suggest a degree of negligence but there is no intention to cause problems. Before a fraud investigation is started, we must rule out simple error. Misuse of resources and misconduct is behaviour that is considered improper when compared with what a reasonable and prudent person would do. Some argue that there is a slippery slope where inappropriate behaviour needs to be challenged. If not, it could accelerate upwards to serious fraud. So overclaiming travel expenses may be seem as harmless fun but it could expand into say more significant crimes, such as fiddling company invoices and worse.

Fraud Can Hurt

This is a true story and is not unusual as businesses in many local communities have taken similar blows.

In one case, a small bakery business employed five local people and prospered in their local community. Several workers decided to defraud the business and sold large quantities of bread on the side by diverting stocks from the main legitimate business. These workers were assisted by the fact that they started baking at four in the morning but the owner did not arrive until many hours later. Eventually, the business crashed owing debts and the local community lost their bakery. The workers lost their jobs and the owner swore he would never invest in a business again.

Fraud Categories

There are many different types of fraud out there and one simple classification has been devised by the Association of Certified Fraud Examiners.

The UK's Fraud Act 2006 created a new general offence of fraud with three ways of committing it:

* Fraud by false representation.
* Fraud by failing to disclose information.
* Fraud by abuse of position.

Fraud Drivers

Frauds can be pre-planned or just opportunist. But they can also arise where someone realizes a system is open to abuse and as we have already said, small scams can evolve into really big frauds. The problem with fraud is that:

- It is deceitful
- It breaches trust
- It normally involves losses
- It may be concealed
- It may appear outwardly respectability

The factors on your right are associated with fraud. If we turn this on its head - the reason we need to be so careful is that if these five things are in place, then fraud will happen. But all frauds involve an element of deception which makes this topic intriguing. The next page contains a warning about fraud and bank staff.

1. Assets or gains that can be exploited
2. Motivation – greed or need
3. Opportunity
4. Sufficient technical ability to breach systems
5. Low risk of discovery or minor consequences of discovery

Fraud and Bank Staff

The National Fraud Intelligence Bureau's (NFIB) Proactive Intelligence Team has become aware of customer services and banking hall staff in retail bank branches being befriended and 'groomed' by fraudsters over long periods of time in order to gain access to personal account data. The intelligence gathered by the NFIB highlights that after being identified by fraudsters, staff are being monitored during their days off and then befriended over a long period of time.

An ex bank employee and now convicted fraudster who is currently serving a prison sentence, has told the NFIB's Proactive Intelligence Team how he was groomed into giving out customer information. The ex bank employee said: 'I used to see them at my local market and they would come up to me and start chatting. It's quite unusual for people to start chatting to you but because of the job we do I guess we are outgoing and approachable. They were nice people. I had no idea they were fraudsters. This went on for a few months before they asked me to do anything. They were really clever and over time they got to know more about me personally'.

Typically, the fraudsters look to exploit the staff member by either offering a financial lump sum for the account information but also by exploiting disgruntled or unhappy staff. The information they require from the staff member is usually customer profile information such as birthdays and maiden names. The fraudsters already have the account number details. The ex bank employee went on to tell the NFIB: 'I had worked for the bank for a few years and maybe I was a bit demoralised. That's no excuse but I think that over time the fraudsters knew this and tried to exploit me'.

'I think that if the awareness training around this was more robust and 'streetwise' then this could be avoided and I wouldn't be in prison. I had no idea that I could go to jail for this. I don't think people realise how serious fraud by abuse of position is. If more people knew that they could go to jail for a couple of years then staff might think twice about getting involved'.

If you believe you are being groomed by a fraudster, please let your employer know immediately and call the police.

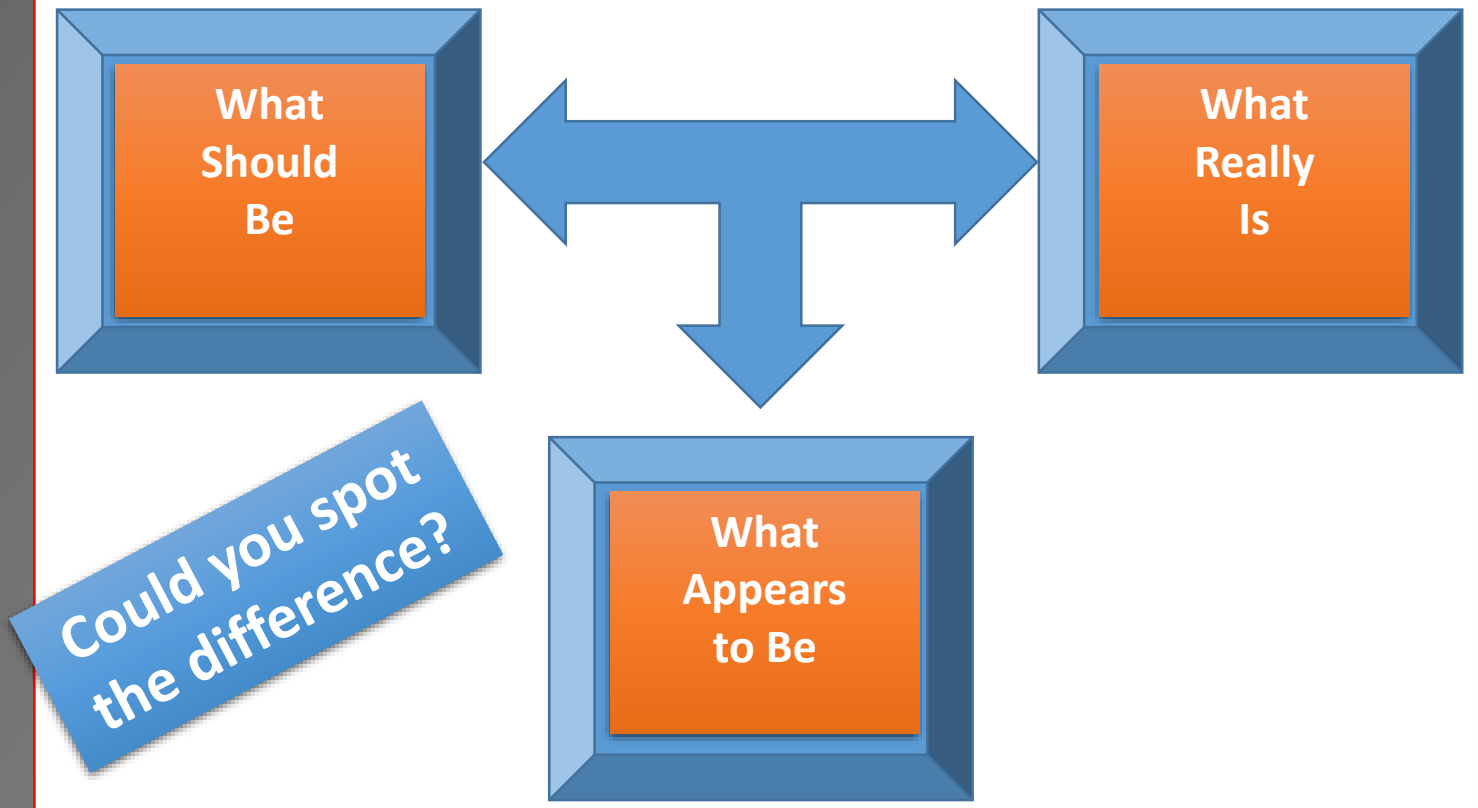
The Art of Deception

Fraud detection arises from being aware of something that does not appear to be right, which means deception.

Have a look at some of the ways you can use to spot the difference. We will explore some of these factors later.

While each fraud is unique, there are some commonalities.

And if you want a short note on different types of fraud, then have a look at the next few pages.



- Odd behaviour
- Complaints from customers
- Altered documents
- Irregular financial statements
- Breach of controls
- Inconsistent information
- Breach of IT security

Types of Fraud (Page 1 of 4)

Travel and Subsistence Claims: This is a common fiddle where claims are falsified, inflated or there is basic abuse of the scheme. Small-scale abuse occurs where people simply overstate their claims. It gets more serious where the claimants put in fabricated sums and may even forge the line manager's signature/authorization.

Cheque Fraud: Where a company cheque is stolen, altered or forged it may be diverted to an unauthorized person who can access the funds and then close the account or simply disappears. Company secretaries and accounts personnel may also be in a position to generate additional cheques and can engage in significant levels of fraud against companies who still make cheque payments.

ID Fraud: This is now a major issue in society. There are many reported cases where people have had to defend themselves against claims, because others have posed using their identity having had access to personal data such as social security number, address, date of birth and so on. An individual can use a stolen ID to defraud banks say by acquiring unsecured loans and credit cards. The costs of re-establishing a reputation that may have been impaired through credit card debt and other bills can be tremendous in terms of both money and time.

Ghost Employees: One well-known fraud is to get extra names onto a company payroll and so divert funds to a bank account specially set up for this scam. If an employee can stay on the payroll having left the company, again extra funds can be obtained for a while. Unauthorized changes to payroll times, rates and claims can result in money being diverted for illegal gain.

Basic Company Fiddles: In these cases, an employee may fabricate sickness to obtain paid sick leave, submit inflated overtime claims, or use company equipment for an unauthorized purpose, such as operating a private business. Where this private business competes with their employer's business, the fraud may also involve theft of ideas and company information such as a client database. A more dangerous development is the sale of information and corporate intelligence that the employee has access to. Pilferage relates to small items taken home by staff. Fabricated time sheets can constitute a theft of time (and so pay) from businesses. What used to be seen as basic fiddles has now become a major problem, as is falsified information on CVs (resumes) from persons seeking employment. In some cases, the person being employed is very different from the person who appears to have the required skills, competencies and credentials on paper.

Misappropriation Schemes: These come in many forms and guises made more difficult by efforts to conceal the nature of the funds lost to the company. Writing off income before it is then received is one concealment technique. Altering sales figures, obtaining blank purchase orders, amending documentation, diverting vendor discounts and writing off balances that are thrown out from account reconciliations are all ways that an employee can misappropriate funds and balance the books at the same time.

Types of Fraud (Page 2 of 4)

Consumer Fraud: These are attempts to coerce consumers into paying for goods not received or goods that are substandard, counterfeit, not as specified, or at inflated prices or fees. The growing use of attractive internet web sites as an alternative to unsolicited phone calls or visits to potential customers, compounds this problem.

Credit Card Fraud: This is another growth area where credit card details are stolen or cloned to be used to secure goods or services in the name of the cardholder. Sometimes, a brand new credit card is obtained using known details. Cards can be stolen or details obtained from files that are not properly secured, while credit card details may also be purchased from people who are able to access this information and even advertise their availability over the internet.

Kickbacks: This generally involves an employee with influence over who gets a particular contract, and who is able to obtain something of value for assisting the prospective contractor. Likewise, bribes may be paid to inspectors to turn a blind eye to substandard goods coming into a loading dock. If these offers of bribes do not work, the dedicated fraudster may well turn to blackmail and threats. Corruption can occur in any type of organization or office. Corruption involves offering, soliciting, giving or accepting inducements which may influence a person's actions.

Bid Rigging: Here a vendor may be given an unfair advantage to defeat the competition for a given contract. A vendor may be provided with extra information to bid low but then raise more income through many variations to the set contract. This may also be linked to the receipt of kickbacks. Election rigging is a similar but more sinister type of fraud.

Inflated Invoices: A company may inflate its bills without agreement from the bill payer who may be a customer. Conversely, an employee may arrange to pay a vendor more than is due in return for an unauthorized payment or some other gain. Also, an employee could pay an amount to an entirely fictitious supplier, and divert the payment to a personal bank account.

Inventory Theft: This is straightforward and involves stealing stock from an employer. It can also involve stealing scrap and goods that are returned by customers since there may be less control over these items. A bigger problem is shoplifting where customers, not staff, steal huge amounts of goods from retail outlets each year.

Theft of Cash: This can arise where cash comes into a company and is diverted. Skimming is where it is taken before it enters the books for example, by a cashier. Embezzlement involves a direct breach of trust where someone entrusted with the cash diverts it for personal use. Lapping is a technique whereby the theft of cash or cheques, is covered up by using later receipts so that the gap in funds is not noticed, sometimes for many years. Some argue that the reported figure for these types of frauds is only around 10% of the actual losses.

Types of Fraud (Page 3 of 4)

Financial Statement Fraud can be very serious and can be used to encourage investment and loans through fabricated or falsified financial figures. Inaccurate earnings figures may also be used as a basis for performance bonuses. Popular frauds involve people buying stock and then 'talking up' the price and selling before the market spots the distortion. Some credit card frauds link into share frauds in that the stolen cards are used to buy stock in the name of the rightful card owner to help boost share prices. Alternatively, a company may be entirely fabricated to attract funding, which, once obtained, disappears from the face of the earth. Where executives or the board are able to fabricate figures and invent performance reports and profits as and when required, then the entire business community is affected. Unfortunately, many an investor has lost out due to this type of fraud. Some indicators of this type of fraud are:

1. Performance pay. Fees and compensation for directors and top management linked entirely to the financial performance of the company.
2. Share price. Tremendous pressure to maintain a high share price and disastrous impact of a fall in the price. Where a director's entire fortune is tied into the value of shares held in the company there is a strong motive to fix things. This would be compounded where the market is in a state of rapid development and high risk venture funding is readily available.
3. Tax bills. Pressing need to keep tax payments low. Financial misreporting not only relates to keeping profits up, but also relates to keeping them down by massaging the accounts.
4. Board oversight. Where there is no real board oversight in place and corporate ethics is seen as a dirty word, then a small group can call the shots with no real control over their activities. In this situation, the audit process is unlikely to have a big impact and the staff may be in fear of losing their jobs, particularly the finance people. There will probably be a high level of staff turnover as people are fired and replaced overnight. There may also be a big gap between staff and managers and no real communication between the board and employees. The only part of the company that works will be the sales team who would fight to meet demanding targets. Where the chief executive and the chief finance officer decide to collude and commit fraud then this can create tremendous problems of misappropriation and concealment.
5. Financial problems. Improper accounting procedures can be associated with poor financial planning and a lack of cash flow. Financial misreporting can cover up fraud by directors or top management. As such an atmosphere of complex inter-company transfers and adjustments may be designed to confuse outsiders. This type of company may well lurch from crisis to crisis, have off shore funds (in tax havens) and many special accounts to ensure a swift exit for the key players in the event of a collapse. There are many signals that fraud is happening. Taken out of context, each individual sign is not in itself significant. But the pattern and combinations that do not add up can lead to an 'at-alert' status.

Types of Fraud (Page 4 of 4)

Cyber Crime: Most organizations are moving away from employee only systems access where users, partners, associates and customers can access their accounts to view and even update their data means sensitive information can be accessed by external parties. These parties are meant to be authorized users and as long as they meet the systems protocols they will be given defined privileges. Since the system believes the user is authorized. Meanwhile people are working away from their offices and are using their own devices, including smart phones to access their work databases and emails. In the same way, customers use their phones to engage with their retail businesses, banks and other service providers. Collaborative working using various shared media is now the norm and most large IT providers have a version of shared links which could hold sensitive data that belongs to a business, whether large or small. The aim is to allow associates to access work areas creating major business opportunities. But alongside these opportunities comes threats from deceitful individuals or gangs.

Computer hacking can be a stepping-stone to securing data, access rights and providing a means to commit fraud. As such, fraudsters may be involved in sabotage, software piracy, stealing personal data, and amending or damaging records held on computer systems. Younger people brought up in a computerized environment can often run rings around their senior managers who do not appreciate the scope for unauthorized transactions inherent in automated information systems. In some organizations staff have more access rights than they need to do their job. Computers can be used to hide transactions but at the same time can capture lots of information on the trail of each transaction.

Control strategies must keep pace with new developments since cyber security is now firmly on the list of top ten risks for most boards of directors in most organizations. Many see Cybercrime as one of the biggest emerging threats for individuals, companies and governments across the world. Future businesses will have to be on-line because of the lower costs, greater accessibility and basic market expectations. The biggest threat is consumers' reluctance to risk their money through for example, credit card transactions over the internet. The sensible business response is to achieve a reputation for reliability and trustworthiness and perhaps seek official recognition in line with set quality standards on information security and data protection. Accepting internal and external abuse and breach of systems security will affect the organization's public reputation. As such, the only way on-line commerce will succeed is for all sectors of the economy to engage fully in the fight against fraud. There is more information on cyber security further on in your Tutorial.

Fraud Categories

As we said, there are loads of different types of fraud out there and loads of ways of committing fraud and staying undetected.

Have a look at these examples and think about ways of categorising each one.

When you turn to the next page try to locate each fraud to a defined category.

- Overclaim business travel costs
- Access data to sell to competitor
- Plant malicious software into corporate network
- Demand cash from supplier in return for a company contract
- Misappropriate cash left in admin office
- Pretend to have a qualification
- Demand money not to tell regulator about irregularities
- Capture personal details of bank customer
- Use company stationery for own business
- Secure funds by abusing position
- Remove small sums of cash from sales income
- Access customer details to obtain credit card

A Question on Loads and Loads of Frauds

Which description goes where?

- Overclaim business travel costs
- Access data to sell to competitor
- Plant malicious software into corporate network
- Demand cash from supplier in return for a company contract
- Misappropriate cash left in admin office
- Pretend to have a qualification
- Demand money not to tell regulator about irregularities
- Capture personal details of bank customer
- Use company stationery for own business
- Secure funds by abusing position
- Remove small sums of cash from sales income
- Access customer details to obtain credit card

BRIBERY	THEFT	SKIMMING	MALWARE
BLACKMAIL SCAMS	EXPENSES FIDDLES	ACCOUNT TAKEOVER	MISUSE OF RSOURCES

An Answer on Loads and Loads of Frauds

How did you get on?

- Overclaim business travel costs
- Access data to sell to competitor
- Plant malicious software into corporate network
- Demand cash from supplier in return for a company contract
- Misappropriate cash left in admin office
- Pretend to have a qualification
- Demand money not to tell regulator about irregularities
- Capture personal details of bank customer
- Use company stationery for own business
- Secure funds by abusing position
- Remove small sums of cash from sales income
- Access customer details to obtain credit card

BRIBERY	THEFT	SKIMMING	MALWARE
Demand cash from supplier in return for a company contract	Misappropriate cash left in admin office	Remove small sums of cash from sales income	Plant malicious software into corporate network
CORRUPTION	MISREPRESENTATION	ESPIONAGE	ID THEFT
Secure funds by abusing position	Pretend to have a qualification	Access data to sell to a competitor	Access customer details to obtain credit card
BLACKMAIL SCAMS	EXPENSES FIDDLES	ACCOUNT TAKEOVER	MISUSE OF RSOURCES
Demand money not to tell regulator about irregularities	Overclaim business travel costs	Capture personal details of bank customer	Use company stationery for own business

Money Laundering

Let's have a quick look at money laundering.

A risk-based approach to money laundering starts with identifying and assessing the risks in question, before devising suitable controls via the nominated officer. In terms of dealing with customers, can you list some of the risks that you should be alert to?

Businesses need to work out how to carry out their risk-assessment, depending of the type of business in question. A simple approach may be appropriate where the focus is on customers who appear to be 'unusual'.

If you want to know a bit more about this topic the next page outlines a few notes.

Money Laundering

Most organizations have a nominated officer and train their employees in how to report suspicious transactions. Criminal activity tends to involve generating large amounts of money. This bulky money has to be 'laundered' since its presence increases many risks for the criminal; such as generating interest from other criminals and from law enforcement agencies. Criminal gangs need to transfer large amounts of cash and money to legitimate funds so that there is no clear trail back to the various illegal sources. Many schemes involve moving money abroad and/or buying assets or investing in businesses that have large cash turnovers. Anti-money laundering procedures mean people doing business with a company need to be able to prove their identity and legality, using suitable documentation such as passports and personal documentation and by providing relevant information. And any suspicious people or suspect transactions or significant/at-risk deals need to be challenged.

What risk is posed by the customers?

For example by:

- brand new customers carrying out large one-off transactions.
- customers that are not local to the business.
- customers engaged in a business which involves significant amounts of cash.
- complex business ownership structures with the potential to conceal underlying beneficiaries.
- a customer or group of customers making frequent transactions to the same individual/group of individuals.
- an individual (or an immediate relative) holding a public position and/or situated in a location which carries a risk of exposure to the possibility of corruption.
- customers based in, or conducting business in or through, a high risk jurisdiction, or a jurisdiction with known higher levels of corruption, organized crime or drug production/distribution.
- transactions that do not make commercial sense.

For information on high-risk countries go to the Financial Task Force website, www.fatf-gafi.org.

A Question

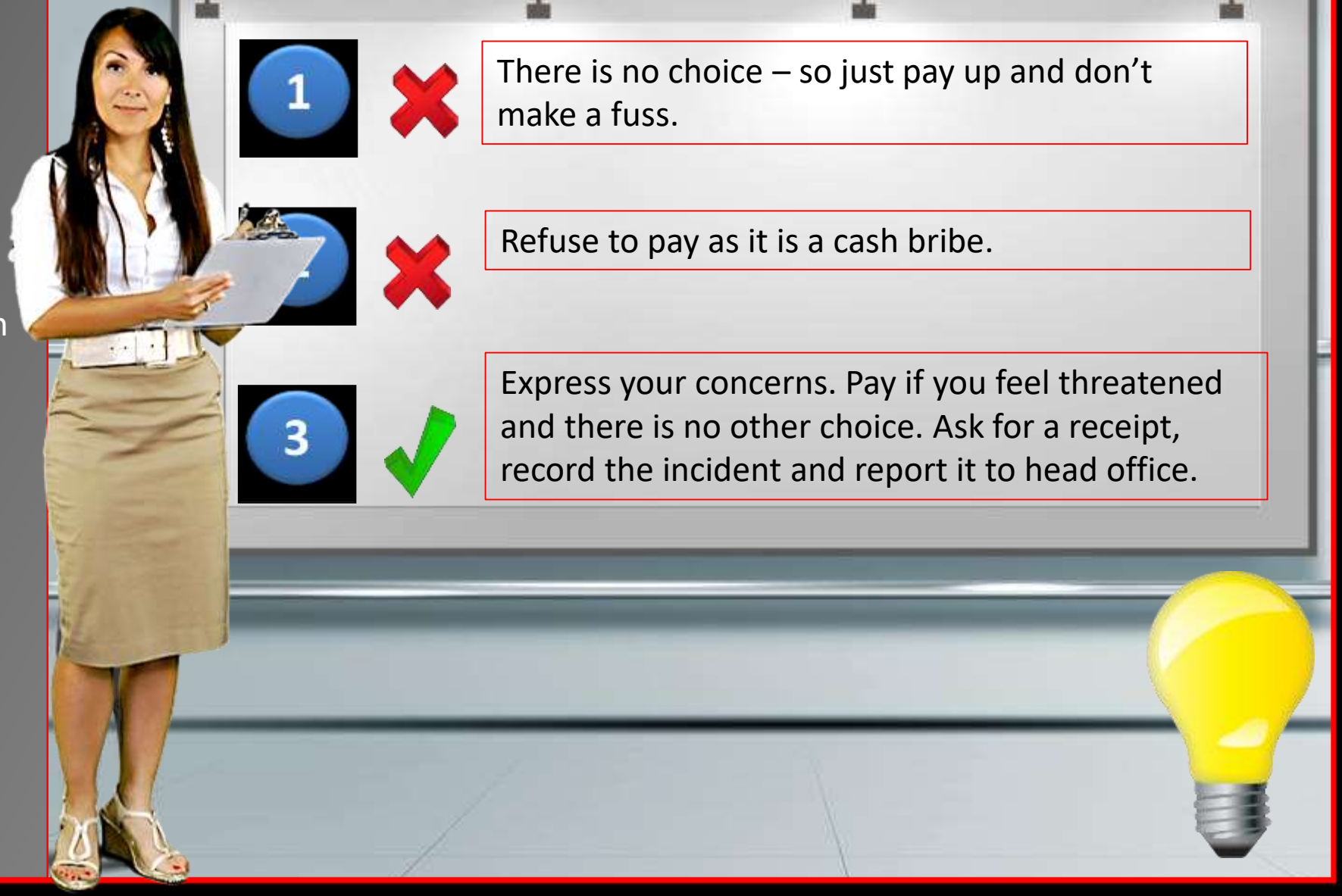
You have just arrived at the airport on your first visit to a remote third world country as part of your exploratory work on checking out new overseas business ventures. As you approach border control a senior security officer takes you to one side and instructs you to give him the 'Business Visitor Arrival Fee'. He makes it clear that you cannot enter the country without paying a cash sum of £500. What is your best option?

?

1. There is no choice – so just pay up and don't make a fuss.
2. Refuse to pay as it is a cash bribe.
3. Express your concerns. Pay if you feel threatened and there is no other choice. Ask for a receipt, record the incident and report it to head office.

An Answer

The Bribery Act 2010 includes the offence of bribing a foreign public official. Which means you need to be very careful when paying over anything to anyone when doing business abroad.
The only real defence is to have adequate procedures in place and have all staff trained in using these procedures. Procedures should fit the types of risks that each organization faces, particularly those working in high risk countries. Sound policies, careful monitoring and zero tolerance with top level commitment are essential.



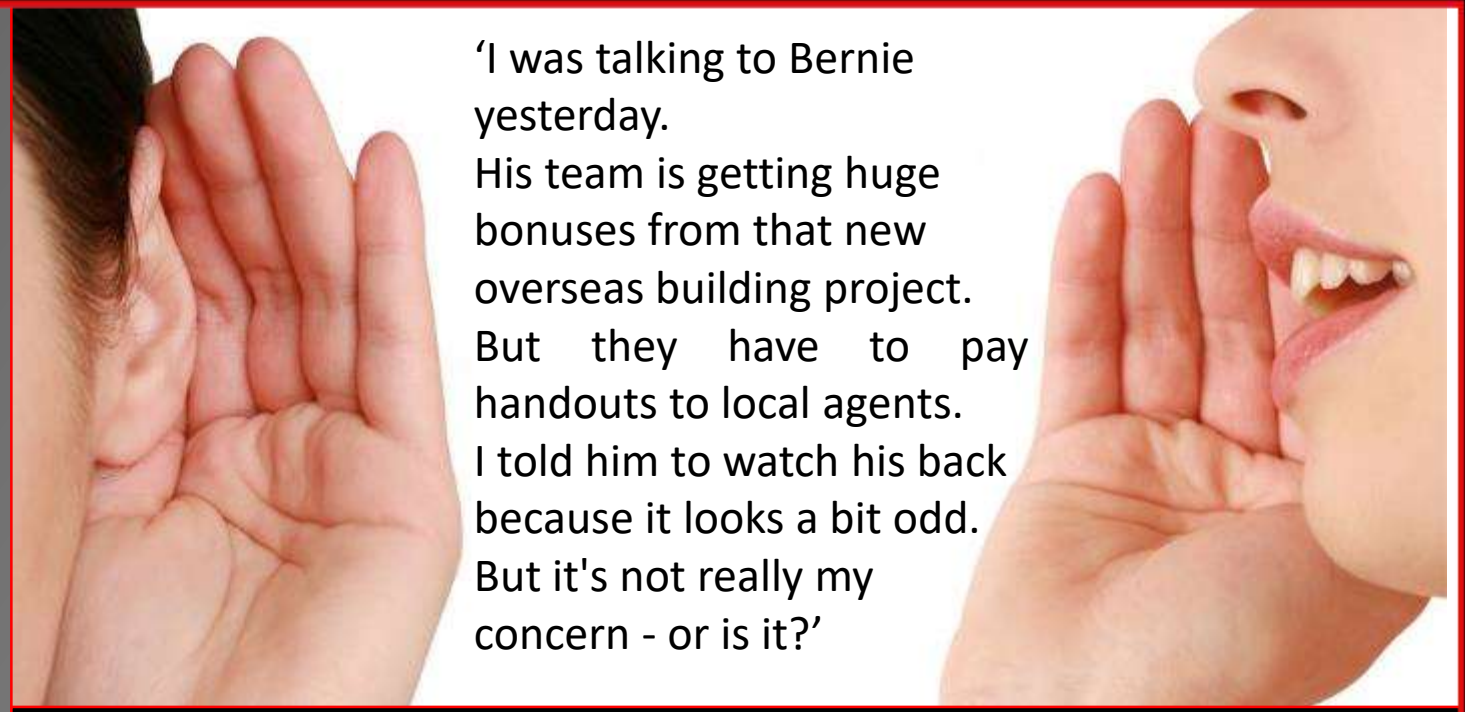
Dealing with Suspicions

Let's explore this idea of bribery.

These types of conversations are going on in the offices of many large companies.

But, what should you do?

We can answer this question by looking at a case study devised by the Ministry of Justice on the next page.



'I was talking to Bernie yesterday.
His team is getting huge bonuses from that new overseas building project.
But they have to pay handouts to local agents.
I told him to watch his back because it looks a bit odd.
But it's not really my concern - or is it?'

Bribery

Ministry of Justice Case study: Facilitation Payments: Case Study

A medium sized company ('A') has acquired a new customer in a foreign country ('B') where it operates through its agent company ('C'). Its bribery risk assessment has identified facilitation payments as a significant problem in securing reliable importation into B and transport to its new customer's manufacturing locations. These sometimes take the form of 'inspection fees' required before B's import inspectors will issue a certificate of inspection and thereby facilitate the clearance of goods. Proposing or including as part of any contractual arrangement certain procedures for C and its staff, which may include one or more of the following, if appropriate:

* Questioning of legitimacy of demands.

* Requesting receipts and identification details of the official making the demand.

* Requests to consult with superior officials.

* Trying to avoid paying 'inspection fees' (if not properly due) in cash and directly to an official.

* Informing those demanding payments that paying the demand may mean that A (and possibly C) will commit an offence under UK law.

* Informing those demanding payments that it will be necessary for C to inform the UK embassy of the demand.

* Maintaining close liaison with C so as to keep abreast of any local developments that may provide solutions and encouraging C to develop its own strategies based on local knowledge.

* Use of any UK diplomatic channels or participation in locally active non-governmental organizations, so as to apply pressure on the authorities of B to take action to stop demands for facilitation payments.

If you want to know more about Bribery have a look at the guide prepared by Transparency International. A powerful quote from the foreword follows:
'Bribery is one of the most recognisable and widespread forms of corruption. A steady stream of corporate scandals and enforcement actions in the UK and abroad show that bribery remains a global problem and a major challenge for companies. But it isn't just companies that suffer. Corruption corrodes the fabric of society. It undermines people's trust in political and economic systems, institutions and leaders. It can affect people's health, money, freedom and sometimes even cost them their lives.'

But why does it happen? Go to the next page for one answer.

IRM and Transparency International UK

Bribery Risk Guide

TRANSPARENCY INTERNATIONAL UK
fighting corruption worldwide

irm

Greed

GREED is the correct answer.

In 2017 it was revealed that a United Nations advisor rigged bidding wars between rival firms and then took some £1.7 million in bribes.

He earned these bribes by telling corrupt firms what the World Bank was looking for in various large scale contracts, working from his home in London. He was jailed for six years and the judge said, 'it was done purely and simply for his own greed and enrichment – he can plead no other motive.'

Before we go to the next part, let me give you a concluding remark.

Business fraud exists, it is causing havoc and it's growing. The best way to tackle a problem is to first recognise its scale and impact.

Your Tutorial

2. DEFINING ROLES

A Question

You go to the local shops to buy a pint of milk and pop into the bank to draw some cash on the way there. While at the bank you check your bank balance and find it contains over £50,000 that you cannot explain. You ask the cashier where the funds came from but she does not know. You return home in a state of confusion.

What would you do next?

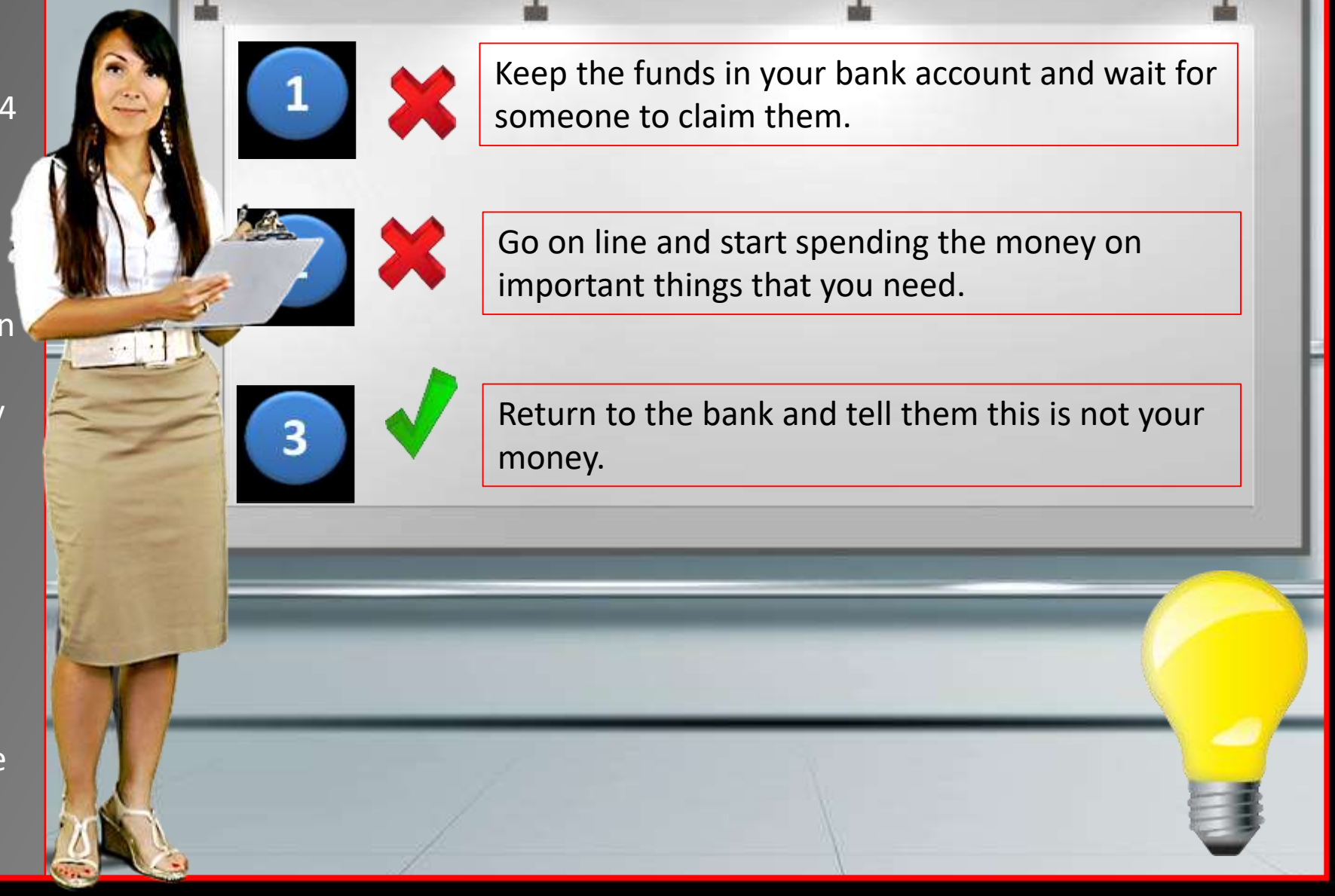
?

1. Keep the funds in your bank account and wait for someone to claim them.
2. Go on line and start spending the money on important things that you need.
3. Return to the bank and tell them this is not your money.

An Answer

Keeping the money is an offence. This actually happened and the culprit was found guilty in April 2014 of dishonesty retaining a wrongly credited bank transfer and was given a 12 months community order - 150 hours of unpaid work. An administrative error meant the local Council accidentally transferred £52,000 into her account. Under the 1968 Theft Act, if you realise money has been paid into your bank account by mistake, you must repay it.

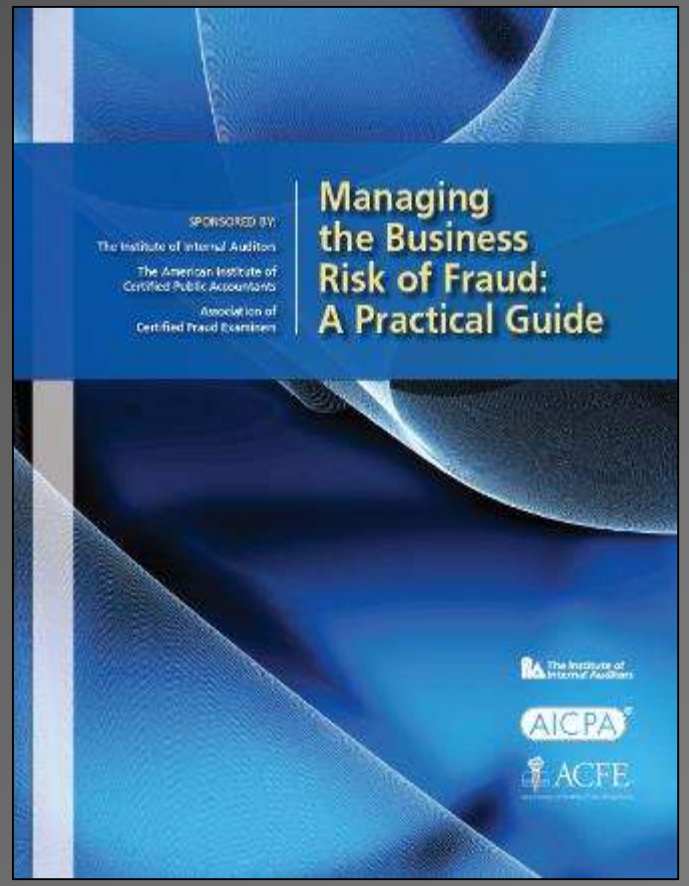
You could commit an offence without realising it.



1. ✗ Keep the funds in your bank account and wait for someone to claim them.
2. ✗ Go on line and start spending the money on important things that you need.
3. ✓ Return to the bank and tell them this is not your money.

Managing the Business Risk of Fraud

A quote for you. An exercise on the next page gives you a chance to think about the different roles for different groups, in terms of fighting fraud.



In addition to the board, personnel at all levels of the organization — including every level of management, staff, and internal auditors, as well as the organization's external auditors — have responsibility for dealing with fraud risk.

A Question on Roles and Responsibilities

Which description goes where?

- Adhere to Anti-Fraud Policy
- Advise on Legal Exposure
- Oversee Anti-Fraud Efforts
- Deal with any Publicity
- Implement & Improve Anti-Fraud Policy
- Alert to Major Fraud During Audits
- Commission the Anti-Fraud Policy
- Advise Management & Investigate Frauds
- Expect Good Fraud Control and Transparency
- Review Fraud Risk Management
- Advise on Staff Conduct

STAKEHOLDERS	MAIN BOARD	AUDIT COMITTEE	CHIEF EXECUTIVE
EXTERNAL AUDIT	INTERNAL AUDIT	ANTI-FRAUD TEAM	PRESS OFFICE
LEGAL SERVICE	HUMAN RESOURCES	MANAGEMENT	ALL STAFF

An Answer on Roles and Responsibilities

How did you get on?

- Adhere to Anti-Fraud Policy
- Advise on Legal Exposure
- Oversee Anti-Fraud Efforts
- Deal with any Publicity
- Implement & Improve Anti-Fraud Policy
- Alert to Major Fraud During Audits
- Commission the Anti-Fraud Policy
- Advise Management & Investigate Frauds
- Expect Good Fraud Control and Transparency
- Review Fraud Risk Management
- Advise on Staff Conduct

If you want more on Roles then have a look at the next page.

STAKEHOLDERS	MAIN BOARD	AUDIT COMITTEE	CHIEF EXECUTIVE
Expect Good Fraud Control and Transparency	Commission the Anti-Fraud Policy	Oversee Anti-Fraud Effort	Ultimately Responsible for Fraud Control
EXTERNAL AUDIT	INTERNAL AUDIT	ANTI-FRAUD TEAM	PRESS OFFICE
Alert to Major Fraud During Audits	Review Fraud Risk Management	Advise Management & Investigate Frauds	Deal with any Publicity
LEGAL SERVICE	HUMAN RESOURCES	MANAGEMENT	ALL STAFF
Advise on Legal Exposure	Advise on Staff Conduct	Implement & Improve Anti-Fraud Policy	Adhere to Anti-Fraud Policy

Respective Roles

The directors act as agents of the owners and they formulate a corporate fraud control strategy in line with stakeholder expectations, and in turn, employ managers and staff to implement this strategy.	The board is responsible for providing an oversight of the way the risk of fraud is managed across the organization. And should set a good example as part of the tone at the top.
The Stakeholders concept recognises the corporate body's wider responsibilities to groups other than their shareholders. It also brings into play the fact that good governance applies to all larger organizations in all sectors.	The audit committee supports the main board by focussing on governance, risk and control. It will be concerned about fraud and receive reports on any significant problems. The audit committee also oversees internal and external audit.
Your organization will consist of executives, managers, supervisors and the workforce who need to manage the risk of fraud and deal with any allegations that may arise from time to time.	The external auditors will be alert to indicators of fraud particularly where this affects the financial statement. Their role has been described more in terms of watch-dogs rather that guard-dogs.
Management hold primary responsibility for the day to day management of all aspects of fraud. It's as simple as that.	Although internal audit are not responsible for fraud control they will provide expertise in reviewing the way management deal with the risk of fraud. Some organizations employ specialist fraud examiners to proactively assist in this task.
All employees need to understand the risk of fraud and the corporate anti-fraud policy. They need to adhere to controls and be alert to, and report any suspicions they might have regarding any potential frauds or irregularities.	What about you? Your responsibility is to understand where you fit into the anti-fraud effort in your organization and do all you can to help fight fraud. Nothing short of showing a Red Light to fraud is acceptable.

Defining Roles

Before we go onto the next part, let me give you a concluding remark.

Everyone who works for, or is associated with an organization needs to pull together to help fight fraud. This is a personal responsibility.

Your Tutorial

3. YOUR PRS CONTEXT

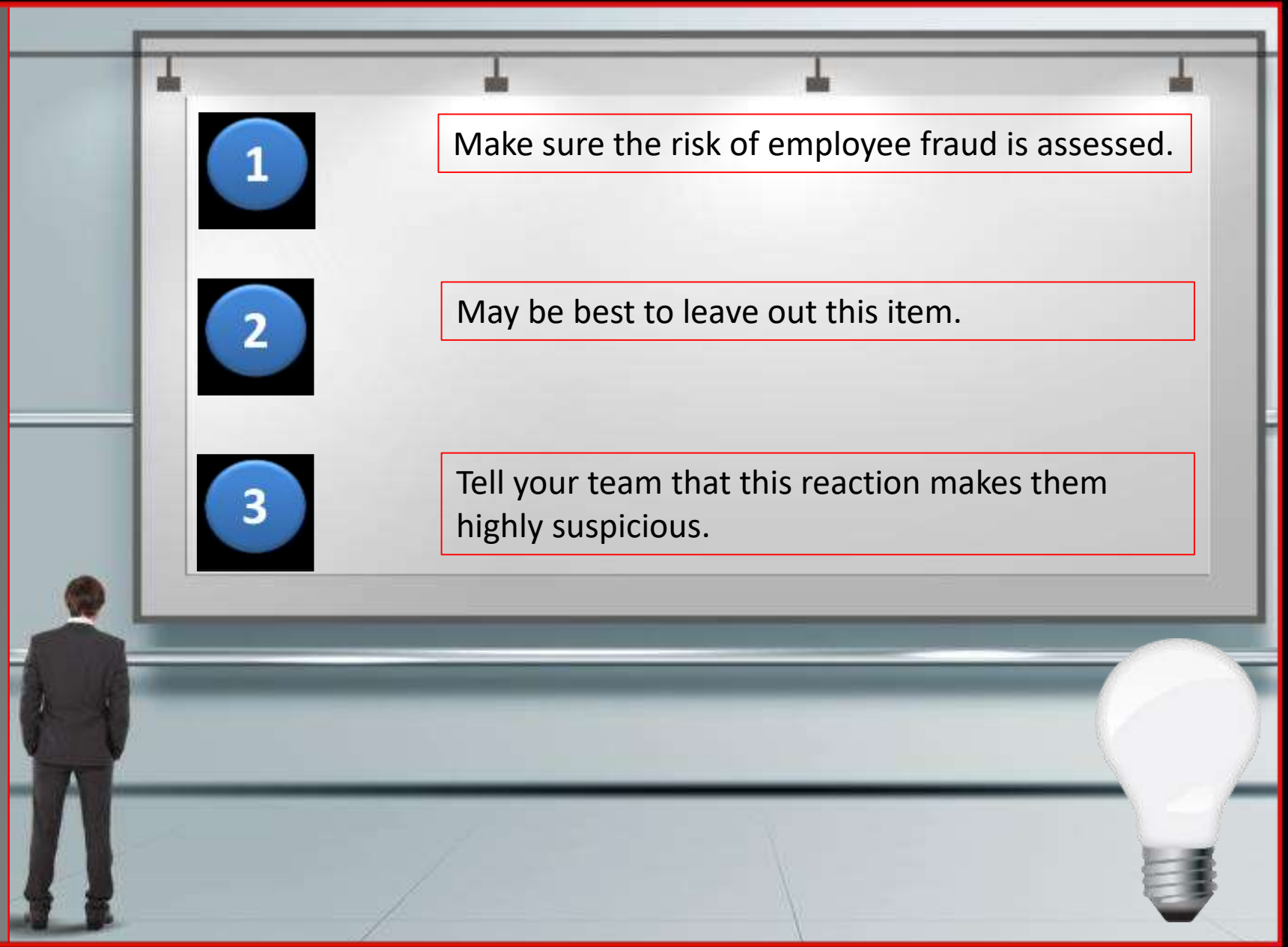
Business Fraud Risk Management

PROGRESS MARKER 35 %

A Question

Your colleagues have been asked to perform a risk workshop to update their risk register after an audit report made this recommendation. Having completed your fraud awareness eGuide you suggest the risk of employee fraud is added to the other risks. Your team members are unhappy about this idea and one of them says – 'does this mean we can't trust each other?' What would you do in this scenario?

Would you chose 1, 2 or 3 as the most appropriate response? The correct answer is on the next page.



An Answer

The best approach would be to tell your colleagues that you do trust them but they would all be vulnerable (and negligent) if your controls were based on all staff being honest, all the time.

So we need to include employee fraud on the risk register.

?

1 ✓ Make sure the risk of employee fraud is assessed.

2 ✗ May be best to leave out this item.

3 ✗ Tell your team that this reaction makes them highly suspicious.

Prevent Respond Stengthen

PRS gives you your role in terms of seeking to help Prevent fraud, Responding if it happens and then Strengthening controls wherever possible.

Your Fraud Policy will give you some insight into these responsibilities and we'll touch on this next.

Corporate Anti-Fraud Policy

Here are some of the items that may be included in a typical corporate fraud policy: Have a look at your own corporate anti-fraud policy and make sure you are happy with its contents.

- Statement of attitude towards fraud
- Personnel policies (e.g. staff vetting)
- Whistleblowing hotline
- Training on prevention and detection (& updates)
- Code of ethics
- Roles and responsibilities
- Procedure where fraud is suspected or discovered
- Link to fraud response plan

Drill Down into PRS

Let's drill down a bit into your Prevent, Respond and Strengthen Controls pointers. Your P, R & S.

It is possible to measure how much employees and associates know about the fraud policy.

If you want to know a bit more, have a look rather than skim past the next page which covers fraud awareness.

Your PRS Role

Your role in anti-fraud activity is to get to grips with the risk of fraud and carry out our three steps (PRS) to ensure you show a red, and not a green light to fraud.

Strengthen Controls

When a fraud happens, this usually means there has been a failure in controls. Which means you and your team need to reassess the way controls operated at the time and quickly improve them. First as a fix to block any further fraudulent activity. Then as a longer term process of re-assessing controls and strengthening them.

Prevent Fraud

You need to have in place sound procedures to prevent fraud. But also be aware of weaknesses that means fraud can still happen. some of these weakness are:

- Absence of controls or lack of security
- Controls by-passed
- Inadequate supervision
- Poor segregation of duties
- Management checks not applied
- Reconciliations not completed
- Collusion.

Respond to Fraud

You also need to have in place a clear way of responding to fraud if and when it should occur. You will need to ensure your organization is able to meet these aims:

- Prevent loss and maximise recovery of losses
- Minimise fraud by rapid action
- Identify the fraudster
- Minimise adverse publicity
- Identify lessons learnt and act on them
- Reduce adverse impact on the business
- Publicise details of prosecutions
- Correct weaknesses in internal controls.

Fraud Awareness

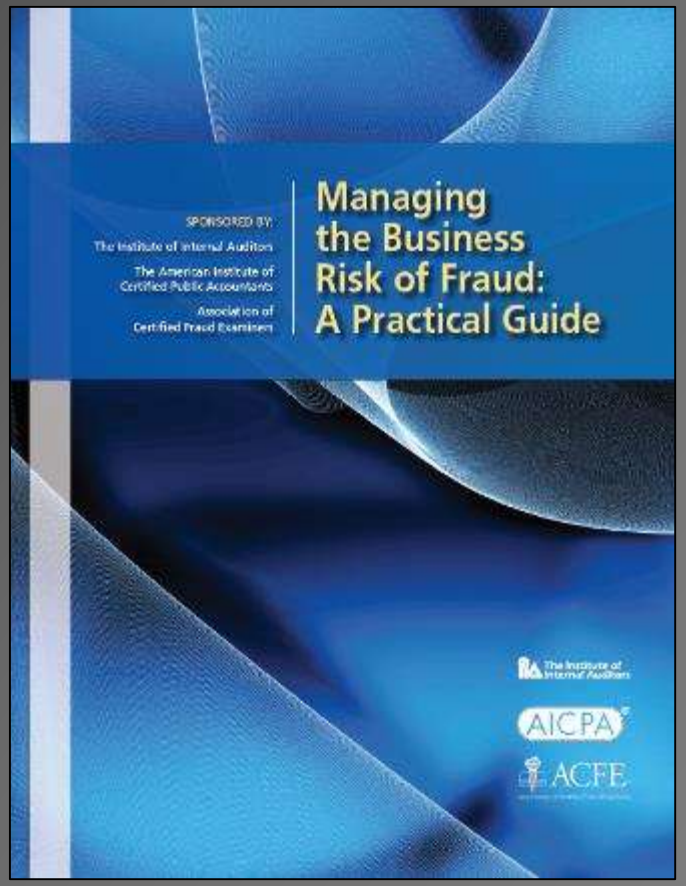
The idea is to encourage staff to Prevent Fraud, Respond to any Suspicions and Strengthen Controls. Herein lies the importance of getting staff to understand and use the fraud policy. Front line staff can represent the best guard against fraud so long as they are alert and inspired to act.

PRS calls for a level of awareness over and above just sending the policy on a staff email. As a start place, measure the level of understanding of the fraud policy around the organization. A simple exercise is to send out a short questionnaire to all staff that asks them to indicate the extent to which they appreciate the organization's position in respect of fraud. Some of the areas that could be covered in such a questionnaire may include the following:

1. Are you aware of the corporate fraud policy?
2. Are you aware of the corporate fraud response plan?
3. Could you access the above documents readily?
4. Are you clear about your responsibilities in respect of fraud prevention, detection and response?
5. Would you know how to react if you received an allegation of fraud? Describe it.
6. Would you know how to react if you suspect that a member of staff was involved in a fraud? Describe it.
7. Are you aware of the aspects of your business that are at risk to fraud?
8. What steps do you take to help manage the risk of fraud?
9. Do your staff have a good understanding of fraud and the corporate fraud policy?
10. Can you suggest any steps that can be taken to ensure the fraud policy is properly understood throughout the organization?

A Likert scale can be used for some of the questions that gives a range of responses from 'None at all,' to 'A lot', or 'Never to Always'. It is best to first pilot the questionnaire in parts of the organization. A small buzz group can also help here to provide feedback to the questionnaire designers. Once the questionnaire is finalized, the idea of taking time out to answer the questions needs to be sold to staff before it can be sent out.

A quote for you. Business Ethics is the cornerstone of the PRS context. If everyone were honest all the time, there would be no fraud. Let's explore this idea over the next few pages.



Effective business ethics programs can serve as the foundation for preventing, detecting, and deterring fraudulent and criminal acts. An organization's ethical treatment of employees, customers, vendors, and other partners will influence those receiving such treatment. These ethics programs create an environment where making the right decision is implicit.

How Honest Are You?

Here is a list of some of things most honest people would not do.

But what about you?

Has your moral compass ever swayed?

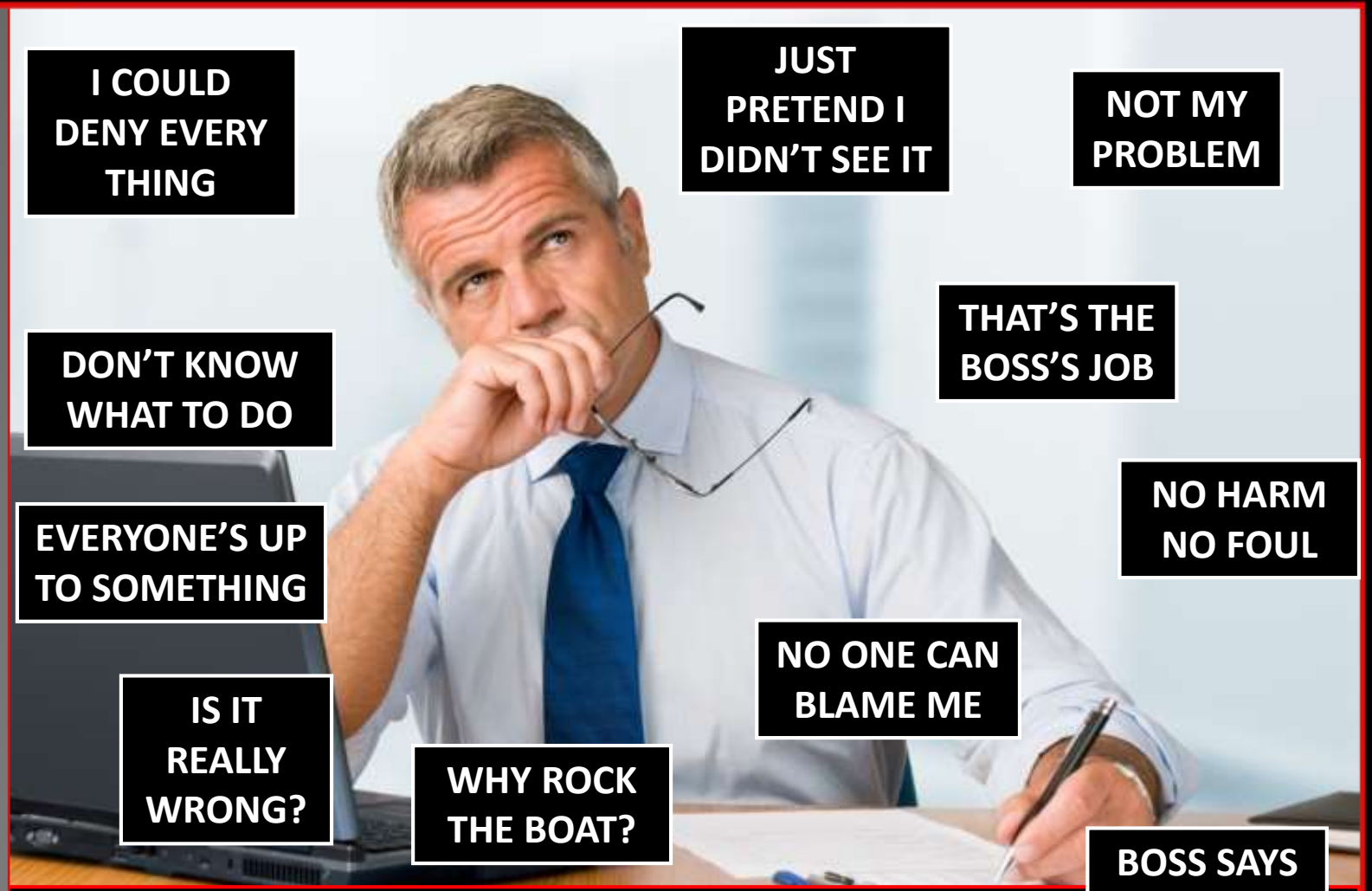
There is the age-old story of a group of business men and women going out for an expensive evening meal after a conference. The restaurant owner approaches them after they have paid for their meal and asks whether they want separate bills for the full amount. So they can each claim expenses, or get tax relief for the cost of the entire group.

Would you ever:

1. Give a personal reference to a friend claiming you have known him for longer than you really have?
2. Join a professional body and quote your membership on your CV without disclosing that you secured membership through experience that meant you did not have to pass the exams?
3. Tell your boss that you made no real contribution to the excellent ideas generated by your team after a recent workshop?
4. Realise some team members were inflating their expense claims and not try to discourage this practice?

Your Moral Compass

Okay- Let's have a closer look at our moral compass. In terms of honesty, things can often become blurred. There are many reasons people pay lip service to ethics. There are also many reasons not to challenge how colleagues behave at work.



Our Moral Compass Should Mean
Everything We Do Should Be:
LEGITIMATE, ETHICAL and JUSTIFIABLE

The Libor Scandal

Ethics underpins the fight against corporate fraud. It is essentially about doing the right thing and assessing the benefits and harm caused by an individual's actions. But this alleged email to a large bank's 'Trader G' in 2006, indicating that some banks had rigged the Interbank lending rate, illustrates how ethical problems can arise.

While back in 2008 Chuck Prince explained how basic company scams, like the 'liar home loans' once started, just keep going on until something is done to stop them.

Chuck Prince, former CEO of Citigroup said:

"When the music stops, in terms of liquidity, things will be complicated. But as long as the music is playing, you've got to get up and dance. We're still dancing."

Ethics and Zero Tolerance

A zero tolerance to fraud is based on everyone, everywhere stressing values that are in place and always observed. Without these values in place, Fraud Control plans simply won't work. But there are times when ethics, although looking good on paper, seems to sit outside the realities of the cut and thrust of business life.

- Be honest
- Be loyal
- Keep all promises
- Disclose conflicts of interests
- Adhere to all policies and procedures
- Be trustworthy
- Be tolerant
- Act with integrity
- Never engage in illegality
- Treat people with respect

What may be possible, is to reset the ethical guide so that it sits inside the working life of employees and associates. Flick between this page and the previous one. Note how you can take the values and add refinements that make them applicable to the workplace – without going into too much detail.

- Be honest and do an honest day's work
- Be loyal to your employer and their values
- Keep all promises and deliver your goals at work
- Disclose actual or perceived conflicts of interests
- Adhere to all policies and procedures and report any violations
- Be trustworthy and provide a safe pair of hand
- Be tolerant of people but do not tolerate apathy
- Act with integrity and protect our corporate reputation
- Never engage in illegality or mislead people even to win business
- Treat people with respect and encourage them to do the same

Your PRS Context

Before we go to the next part, let me give you a concluding remark.

Fighting fraud starts with promoting integrity. This is much harder than you think when the lines that should be drawn are not always clear.

Your Tutorial

4. FRAUD RISK MANAGEMENT

A Question

You have been asked to make cuts to your recruitment team and your manager suggests you do not replace David, who is leaving. David carries out detailed checks on references and qualifications for all new recruits. Your manager says, there have never been any problems with new staff so this check is a waste of time. What would you do in this scenario? Would you chose 1, 2 or 3 as the most appropriate response? The correct answer is on the next page.

?

1. Discard the checks.
2. Retain the checks.
3. Discard the checks but keep an eye on new recruits.

An Answer

You should retain the checks. Staff vetting is a key anti-fraud control as criminal gangs are starting to 'plant' employees into organizations. Which means it should not be discarded.

1 ✗ Discard the checks.

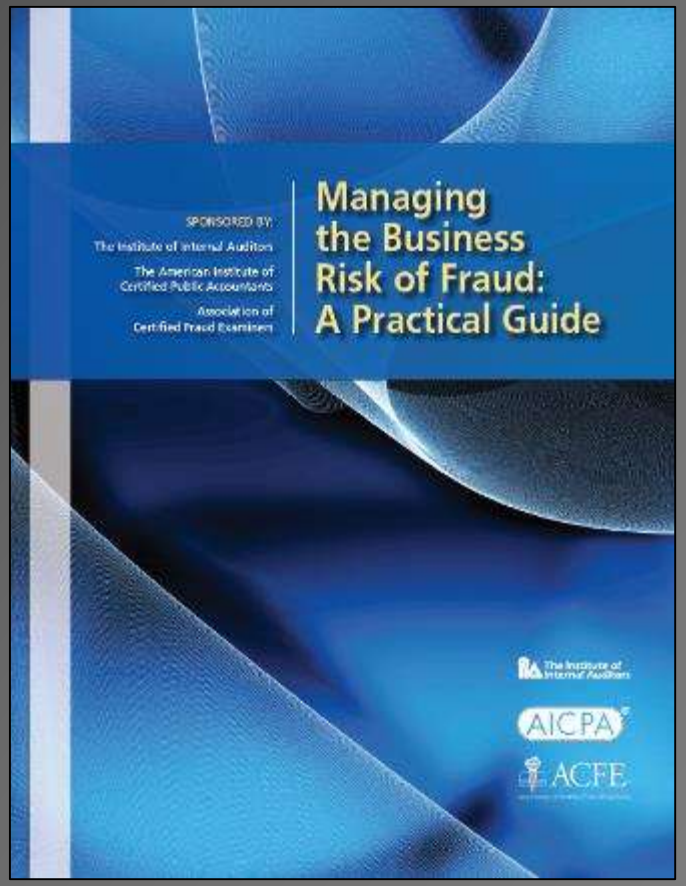
2 ✓ Retain the checks.

3 ✗ Discard the checks but keep an eye on new recruits.

?

Managing the Business Risk of Fraud

A quote for you. The next page will show you how some organizations deal with fraud.



To protect itself and its stakeholders effectively and efficiently from fraud, an organization should understand fraud risk and the specific risks that directly or indirectly apply to the organization. A structured fraud risk assessment, tailored to the organization's size, complexity, industry, and goals, should be performed and updated periodically.

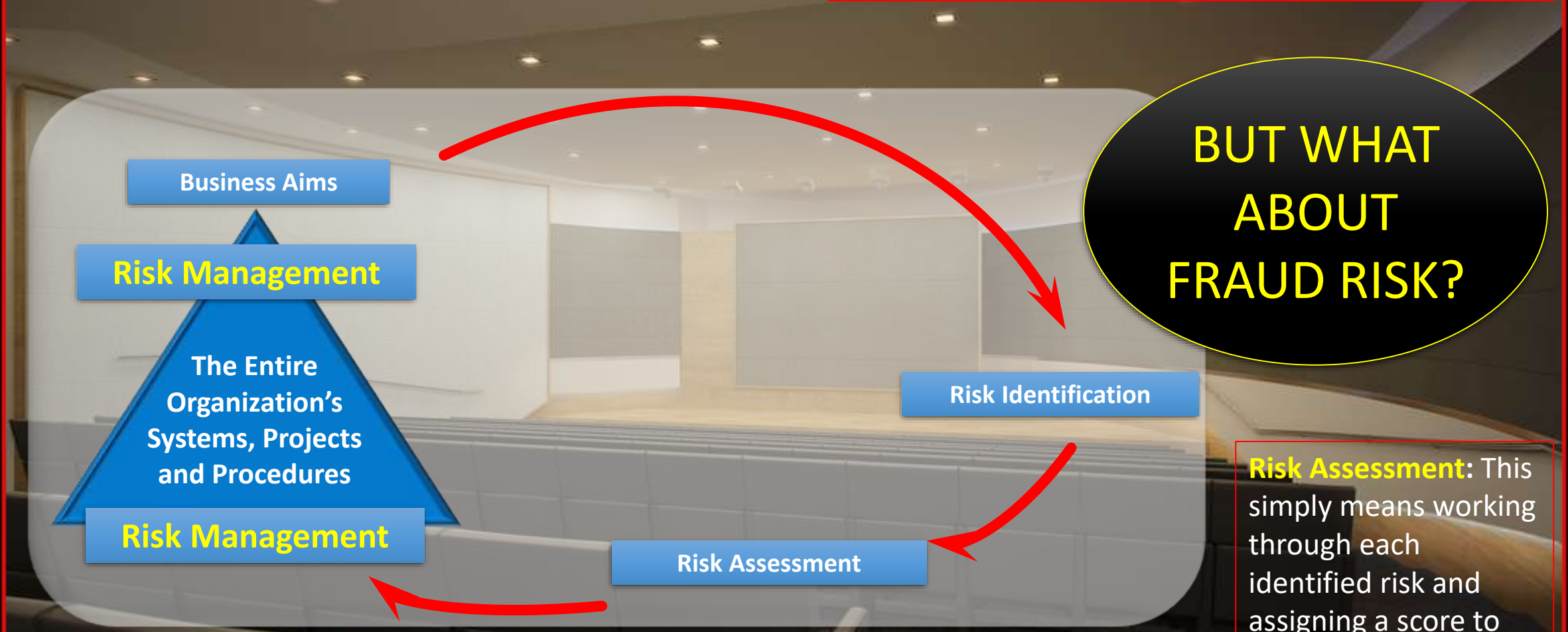
Protect Your Business

Many organizations approach fraud control by relying on the fact that the fraudsters cannot get everyone. With luck - they will escape being attacked. This is simply not good enough. Business Fraud Risk Management needs to be properly planned by everyone pulling in the same direction.

Let's go over the basic risk cycle next, then get this idea of fraud risk onto the agenda.

Business Aims: Start with business aims so that risks are seen as anything that impacts the ability to get results.

Risk Identification: Then consider risks in your area of responsibility.



BUT WHAT ABOUT FRAUD RISK?

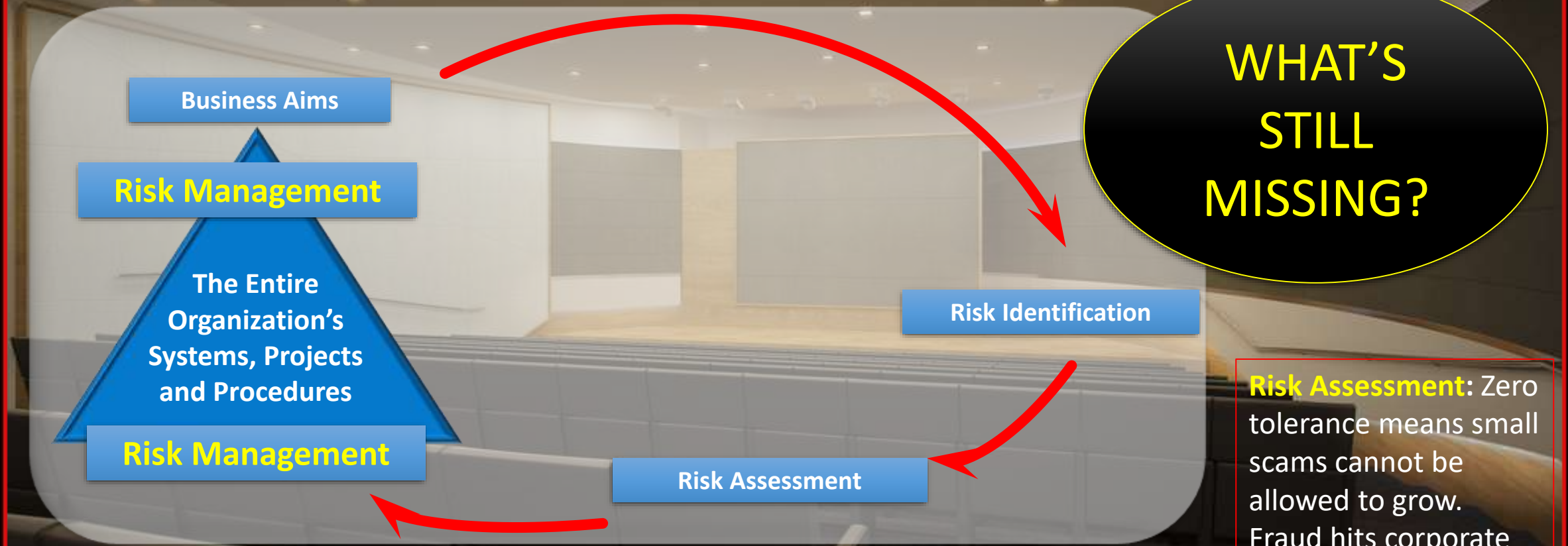
Risk Assessment: This simply means working through each identified risk and assigning a score to reflect their relative importance.

Risk Management: The next stage is problem solving where teams isolate measures to mitigate key risks that are judged to have an important impact on business success.

Fraud Risk Management

Business Aims: Ensure staff can see where fraud prevention fits with their overall objectives. Where the organization ignores fraud issues and writes off any losses, fraud risk management is doomed.

Risk Identification: The problem is, fraud involves deceit so any violation may not be evident. New frauds can be inventive and very hard to anticipate.



WHAT'S STILL MISSING?

Risk Assessment: Zero tolerance means small scams cannot be allowed to grow. Fraud hits corporate reputation and must be prevented.

Risk Management: The most effective control of fraud is alert staff who understand the risks and how controls are important. Data analytics and whistleblowing are crucial tools.

Fraud Risk Management

Business Aims: Ensure staff can see where fraud prevention fits with their overall objectives. Where the organization ignores fraud issues and writes off any losses, fraud risk management is doomed.

Risk Identification: The problem is, fraud involves deceit so any violation may not be evident. New frauds can be inventive and very hard to anticipate.

Review: Your risk reviews provide a chance to get to grips with a fast changing environment where threats such as cyber crime are growing.

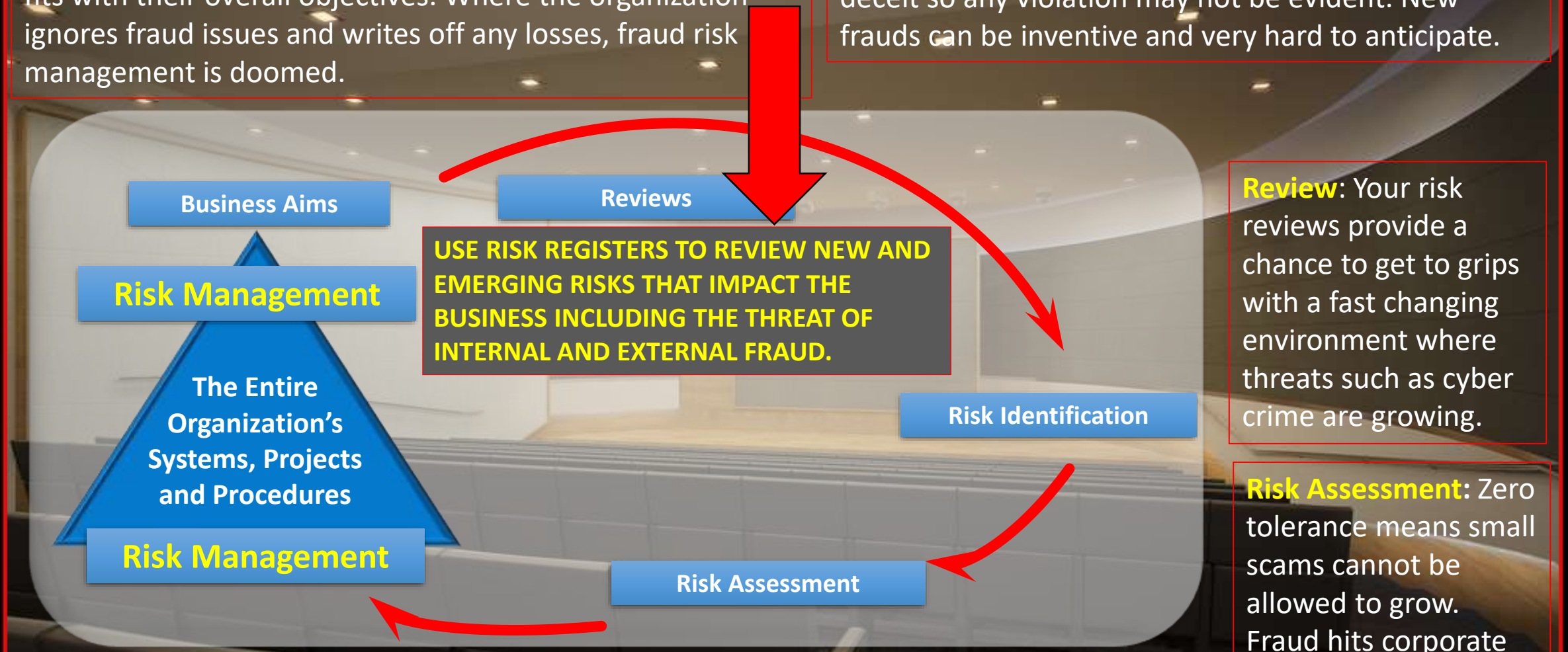
Risk Assessment: Zero tolerance means small scams cannot be allowed to grow. Fraud hits corporate reputation and must be prevented.

Risk Management: The most effective control of fraud is alert staff who understand the risks and how controls are important. Data analytics and whistleblowing are crucial tools.

Fraud Risk Management

Business Aims: Ensure staff can see where fraud prevention fits with their overall objectives. Where the organization ignores fraud issues and writes off any losses, fraud risk management is doomed.

Risk Identification: The problem is, fraud involves deceit so any violation may not be evident. New frauds can be inventive and very hard to anticipate.



Review: Your risk reviews provide a chance to get to grips with a fast changing environment where threats such as cyber crime are growing.

Risk Assessment: Zero tolerance means small scams cannot be allowed to grow. Fraud hits corporate reputation and must be prevented.

Risk Management: The most effective control of fraud is alert staff who understand the risk and how controls are important. Data analytics and whistleblowing are crucial tools.

Your Risk Register

We suggest the use of Risk Registers, or risk logs to help identify and fight fraud.

This is what a basic risk register might look like.

The next page explains each column.

Unit	Objectives							
Ref	Risk	Impact	%	Score	Risk Mitigation	Risk Owner	Date	Review KPI
Risk 001								
Risk 002								
Risk 003								

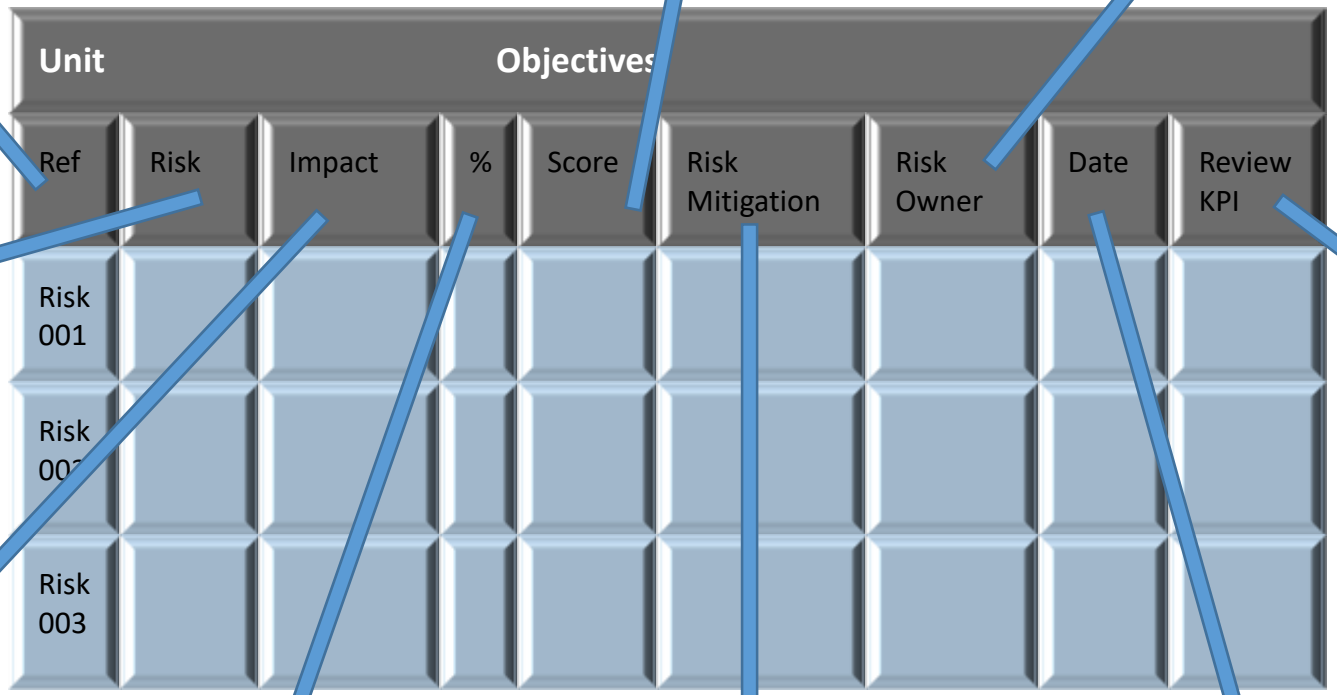
Your Risk Register

Here you go.

Cross referenced to source of risk assessment. For example, from a near-miss report

The way the risk is rated using its impact and likelihood (%)

The person who is responsible for the required action



The risk that has been identified

Action required made into a key performance indicator

The effect the risk would have if it materializes

The probability that the risk will materialize

Action that should be taken to manage high priority risks that impact the objectives

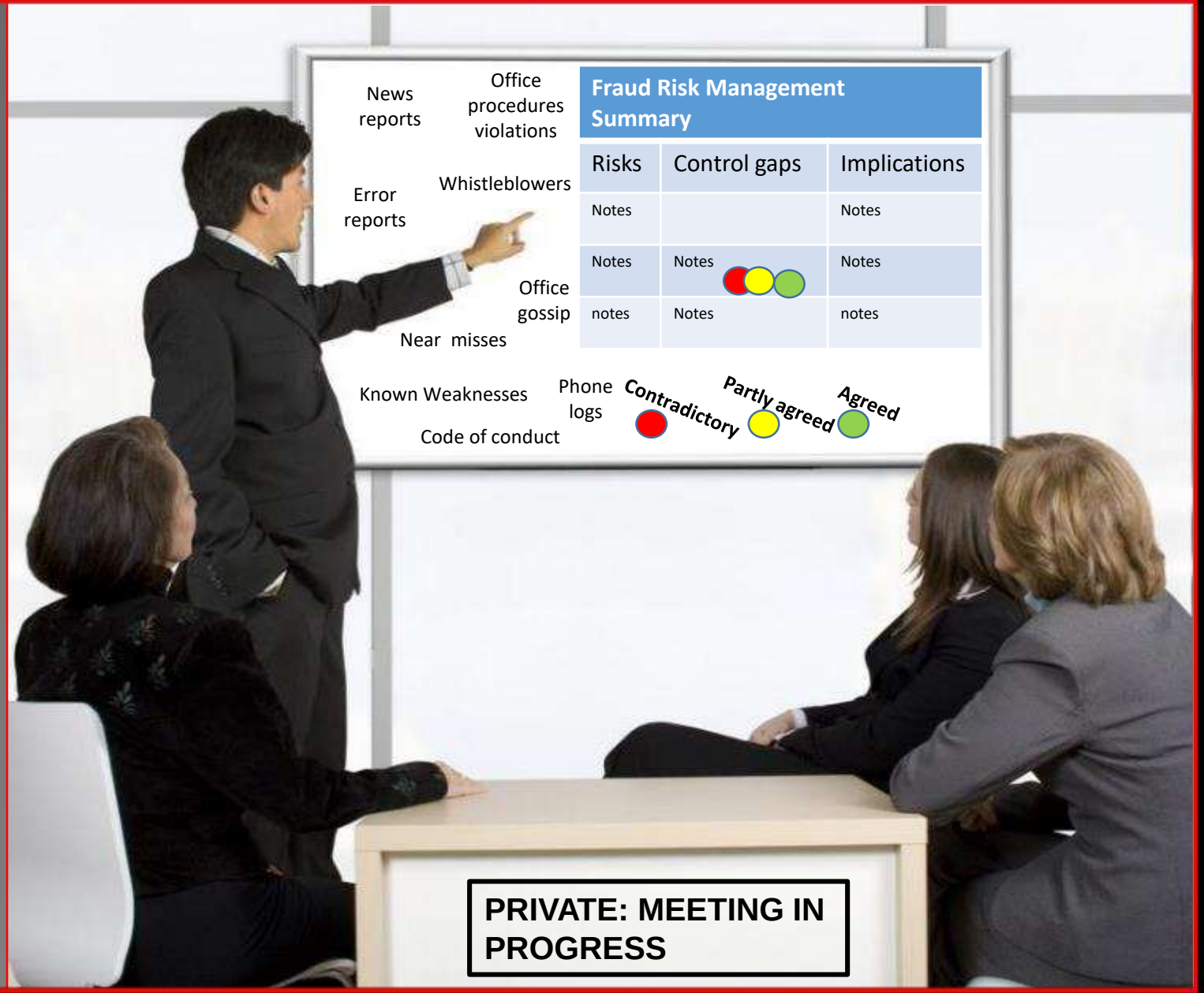
When the mitigation will be implemented.

Fraud Risk Management – Team Work

Whenever your team get together to discuss controls and whether they work properly, make sure fraud is on the agenda. And ask searching questions on whether you are doing enough, including:

- Is there anything we're missing?
- Are we sure everyone is sticking to the right procedures?
- Could we ask internal audit to do some more work here?
- How about running some data analytics to uncover oddities?
- What about that fraud in company x? Could anything like that happen to our company?

And consider the risk of fraud in conjunction with your controls. The next page lists some more questions you might want to consider.



WHAT ARE THE RISKS?

- What would be the impact of a fraud in my area?
- What frauds have we had in the past and why?
- How could my staff perpetrate a fraud?
- What problems have occurred in other similar operations/companies?
- What parts of the operation are open to abuse?
- What are my staff telling me about potential concerns?
- What have I read in the press about new frauds that could affect me at work?
- Is there anything that is worrying in terms of inconsistent activities?
- Are there parts of the operation where procedures are being breached?
- How could our systems be breached by people outside the organization?
- Is there any way that I could commit a fraud against the company?
- Are we taking the threat of fraud seriously?
- Is there anything else we should be doing at work?

WHAT ABOUT OUR CONTROLS?

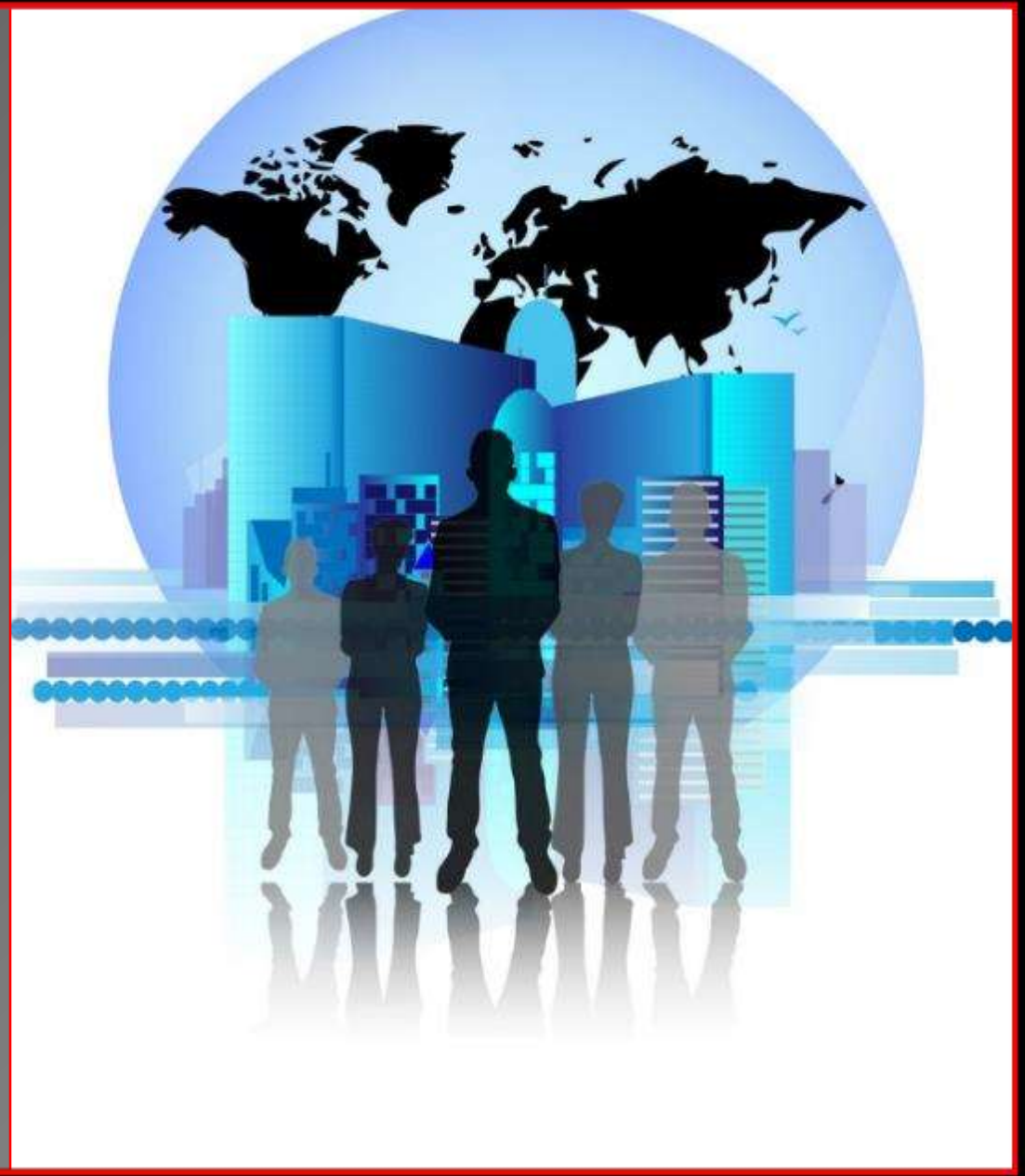
- How important is this control?
- When was it last reviewed?
- Is the control clearly defined and properly set out?
- Do staff understand the control and its importance?
- Does this control work in practice?
- Is the control being by-passed at all, and if so why?
- Should our team receive some training in controls compliance?
- Should we prepare some 'Desk Notes' as reminders of the key checks?
- What are my auditors telling me about weak controls?
- Does the control address all the known fraud risks that it is meant to deal with?
- Can I double-check a few transactions to ensure the control is doing what it is supposed to do?
- What is my overall assessment and do I need to make any improvements?
- Can I issue formal assurances to my manager on the adequacy of the control?

Cyber Security

We cannot leave this idea of assessing fraud risk without mentioning Cyber Risks. And the need for good cyber security.

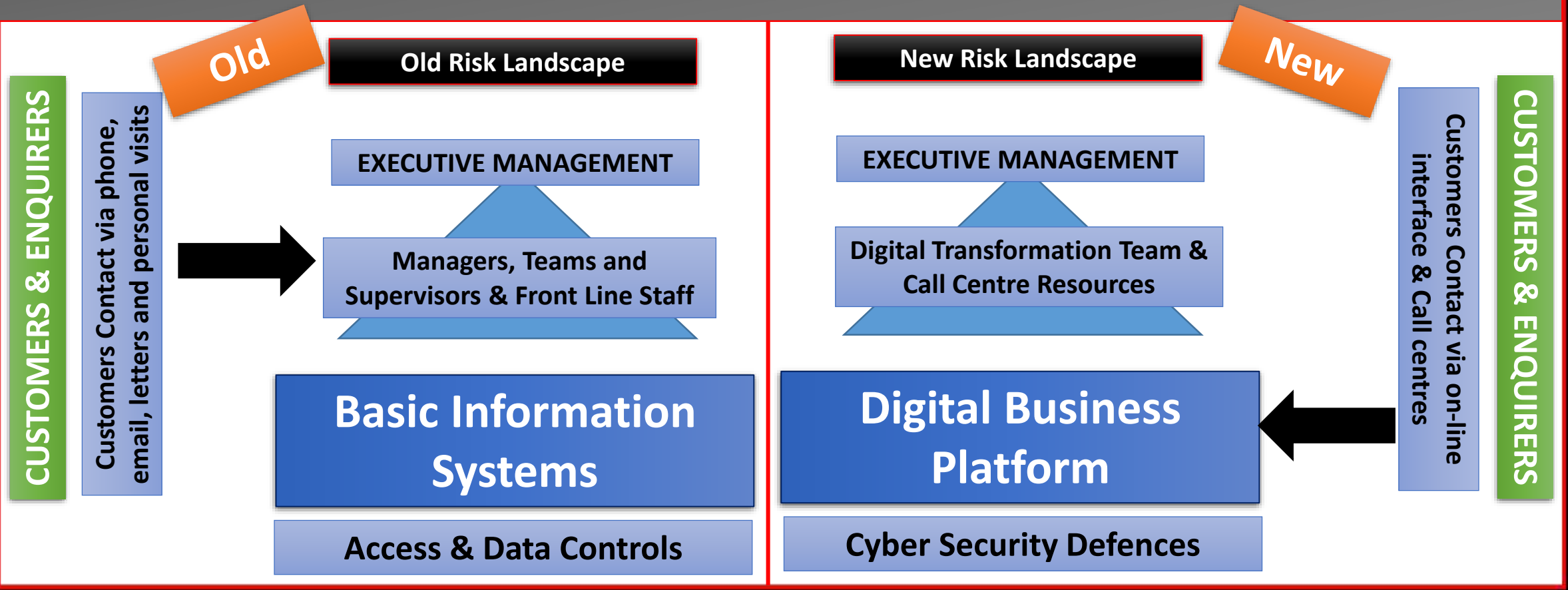
The next page provides two simple models that give one explanation of the way business models are changing to mean cyber crime is now such a growing risk.

The models show the old risk landscape on the left and the new one on the right. Turn to the next page and have a look.



Warning - New Age Business Fraud

Fraud like any other risk changes as the risk landscape evolves and old business models quickly transform into new businesses where the customer interacts directly with the business as well as via front line teams. Customers are getting used to working with automated processes and accessing their personal accounts to amend data, make payments and authorize their own transactions. This is where cyber fraud comes to the fore where criminals can use the Digital Platform to commit fraud. Cyber security is now a key control to stop outsiders gaining unauthorized access which needs to be assessed and reassessed on a regular basis.

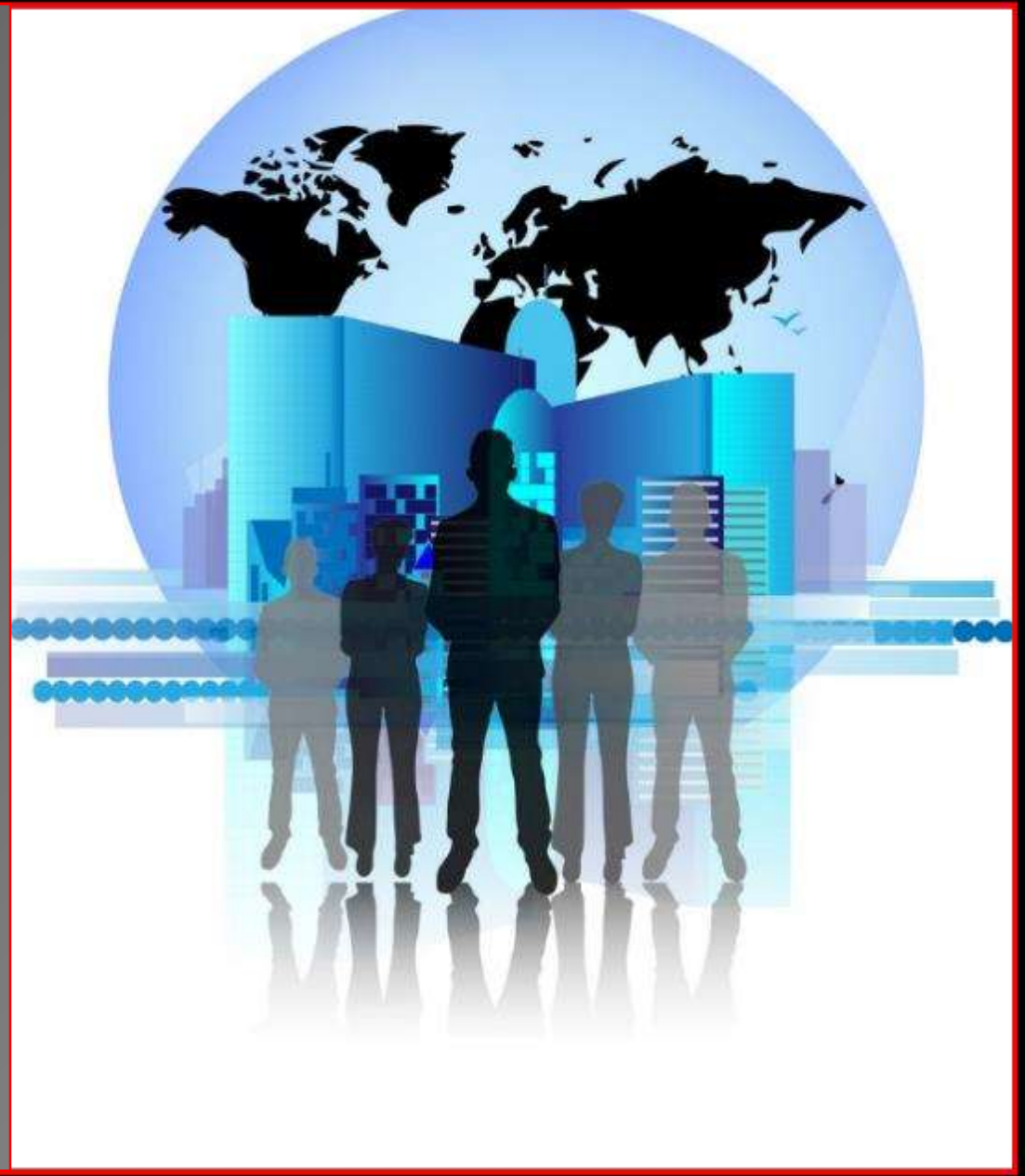


Cyber Security

Here are some questions about this risk that may be included in your assessment:

1. What type of risks are coming on line?
2. How do these risks materialize?
3. What are our legal obligations?
4. What do these risks entail in terms of impact on operations and the likelihood that they will materialize?
5. What does the IT security strategy currently do about these risks?
6. What do we do when there is an adverse event?
7. How can we stay on top of things?
8. Is our entire workforce mobilized against these new and emerging threats?
9. Do we need more awareness, resources and expertise to tackle these threats?
10. Where do we stand in terms of our competitors in the way we are meeting these new challenges?

If you want more on this topic then have a look at the next six pages. If not, just skim through these pages.



Cyber Security (Page 1 of 6)

The unstoppable growth in e-business means rules on encryption, third party access and bring-your-own-device, are all important as information control strategies must keep pace with new developments. Cyber security is now firmly on the list of top ten risks for most boards of directors in most organizations.

All organizations needs to keep up to ensure that they have control over complex new systems that are streamlined, fast moving and open to abuse - in terms of hacking, ransomware, data error and even lost data, if not properly protected. Information that is used over networks can be hacked. Since most organizations are moving away from employee only systems access where users, partners, associates and customers can access their accounts and view and even update their data means sensitive information can be accessed by external parties. These parties are meant to be authorized users and as long as they meet the systems protocols they will be given defined privileges. Since the system believes the user is authorized.

Meanwhile people are working away from their offices and are using their own devices, including smart phones to access their work databases and emails. In the same way, customers use their phones to engage with their retail businesses, banks and other service providers. Collaborative working using various shared media is now the norm and most large IT providers have a version of shared links which could hold sensitive data that belongs to a business, whether large or small.

The aim is to allow associates to access work areas creating major business opportunities. But alongside these opportunities comes threats from deceitful individuals or gangs. The response to cyber risks will be the very same as other risks in terms of the way they should be addressed.

In May 2017 so called 'Wannacry' hackers broke into 230,000 computers owned by the UK's National Health Service. The hackers used ransomware to encrypt files so they could no longer be accessed. They then demanded a fee to unlock these files as a form of blackmail.

Cyber Security (Page 2 of 6)

We can consider cyber security by encouraging the board to ensure the organization is able to address ten basic questions:

1. What type of risks are coming on line?

We have already mentioned some of the risks with networked systems and cloud computing is another area where organizations have no physical security over their data since it resides on-line - but also sits on someone's desktop computer and is backed up remotely. Encouraging customers to access and update their personal data without intervention from staff is now the norm in many organizations and again there are risks in assuming only authorized people can get into the systems. Threats such as ransomware, malicious software hidden in email links and botnets that launch denial-of-service attacks are now much more frequent. They may be general or targeted to a particular organization where cyber-crime and even cyber-espionage can raise its ugly head. On a wider front, cyber-warfare is something that all governments are concerned about as cyber security merges with national security. And there are the obvious links to out-and-out terrorism. A dangerous, if less severe threat arises where these coordinated cyber attacks are aimed at undermining governments or political parties or even seeking to influence an election. Corporate networks and internet connections create risks to cyber security that must be understood and managed. Cyber security is now a huge concern as one case involving the US based consumer credit agency, Equifax found when a cyber attack in July 2017 affected some 143 million customers. The firm immediately employed a cyber security expert and referred the matter to the police.

2. How do these risks materialize?

This question is about keeping up to date with the latest techniques used by external players as they attempt to hack systems or cause disruption to business operations through say denial of service attacks. A risk is only a risk if it is known about and as criminals become more sophisticated, the perfect crime is committed in a way that means it is not detected at all. Some hackers target organizations who are seen as unethical or who have been involved in a scandal that stimulates protest groups to take direct action to undermine them. Corporate assets such as corporate and personal data, services, goods and finances are all at risk if they can be accessed by unauthorized parties.

Cyber Security (Page 3 of 6)

3. What are our legal obligations?

The laws and regulations on data privacy mean organizations can be fined or sanctioned by allowing unauthorized access or holding inaccurate data. This means corporate policies should make clear what 'can' be done, what 'should' be done and what 'must' be done in terms of the way their information systems are used and ensure there is good compliance. There may also be a legal requirement to perform due diligence on companies who are being used as business partners before sharing sensitive data with them. The General Data Protection Regulation will hit the UK in 2018 and tightens up many requirements including the need to ensure consent from individuals whose data is held, along with tougher fines for non compliance with new rules on the way data is stored and used and how breaches are reported.

4. What do these risks entail in terms of impact on operations and the likelihood that they will materialize?

This is the basic risk assessment that should be ongoing. Frequent vulnerability assessments and threat identification should be undertaken and a consideration of risks such as bugs that are not being fixed properly or speedily. One useful policy is to prioritise security controls when undertaking change programs and updates that allow malicious code to get in, as this is often where problems creep in. Whenever a system is updated it should not be signed off until it has passed a cyber security review.

5. What does the IT security strategy currently do about these risks?

Control Objectives for Information and Related Technology (COBIT) is a framework created by ISACA that enables managers to bridge the gap between control requirements, technical issues and business risks. Many companies are now revamping their cyber security strategy as part of their overall IT security strategy. After customer data was stolen from the Cex online games store which affected up to two million customers, the retailer urged customers to change their passwords. Although the stolen credit card details were encrypted and likely to have expired. In a statement made in August 2017 the company said it had employed a cyber-security specialist to review its systems to prevent such a 'sophisticated breach' from happening again. Some frauds are very old fashioned and do not rely on cyber breaches at all. For example, a British Broadcasting Corporation reporter posed as a Royal Mail postman in 2017 and discovered a fraud where postal workers were being offered £1,000 a week to steal letters containing credit cards. Some 1,759 Royal Mail workers were convicted of theft between 2007 and 2014.

Cyber Security (Page 4 of 6)

6. What do we do when there is an adverse event?

The best laid plans can still mean a breach occurs. And it is the way management deal with this breach that could well determine whether the corporate reputation remains intact, or even enhanced. A sound Business Continuity Management Plan is a good start place for dealing with cyber security breaches. There will need to be a rapid incident response plan that swings into action that involves tasks such as:

- Task force swings into action. Including the Chief Information Officer, risk owners and other nominated people.
- Infected areas quickly isolated. Network segmentation and firewalls will help here so that all at-risk parts can be closed down or suspended.
- Impact on finances, health & safety, legal compliance, critical business processes, assets and overall reputation should be assessed.
- Associated systems and media scanned while back ups are checked and the business continuity plan is applied.
- Access controls suspended, reset and reissued - say passwords and other devices.
- Consideration of whether any staff or associates have been compromised and appropriate action taken.
- Communications with suppliers, partners, associates and others who need-to-know.
- Systems and linked devices disinfected and relevant media sanitized and then reset or reinstated.
- Incident reports prepared and all official parties notified. Fines may be increased where a company tries to cover up a breach.
- PR exercise to report problem to users and media outlets in a proactive way with consistence messages and all staff aware of their response. The CEO of Equifax who were hacked in July 2017 spoke on a video about the response to this hack saying he should be judged on the response to this major problem.
- Control fixes quickly put in place to make sure one slip is one too many and the door has been firmly closed to future attacks.
- Longer term solutions created after the matter has been investigated and a review of whether the response was good enough.

7. How can we stay on top of things?

In one sense, cyber security can be seen as an ongoing battle. Companies and other entities seek to strengthen their defence while hackers devise more and more sophisticated ways of breaching these defences. The goal is to invest in keeping these defences strong and deterring would-be attackers so they look for weaker targets. A focus on access control is key to good defence and there should be a detailed record of who has access to what, for how long and who authorized it as well as records of access patterns and inconsistencies.

Cyber Security (Page 5 of 6)

8. Is our entire workforce mobilised against these new and emerging threats?

There should be a clear ownership of cyber risks at the highest level and leadership that pushes key messages down to the entire workforce. This has a lot to do with the culture in place where personal information is seen as important and the need to protect it is fully recognized. One weak point in the system is where some staff allow access or do not challenge odd requests/patterns, that can be exploited by the cyber criminal. Cyber risks do not only relate to corporate networks but they can also arise where work phones, video conferencing systems, smart TVs, Bluetooth and mobile devices, smart phone emails/messages and faxes are hacked and sensitive data obtained by unauthorized parties. The entire workforce should be told that they must guard their workstation and observe screen locks, password controls, use of mobile phones to photograph screens, shoulder surfing and anything else that may compromise data security. A workstation may be redefined as any access point wherever located and through whatever device the employee is using. Another high risk area is privileged accounts access for senior staff and here more controls and more monitoring is required to ensure these facilities are not abused. One solution is to employ a board level Chief Information Security Officer who is properly aligned to the business role of the entity since IT is no longer a device that sits in the basement. It is a strategic resource, brimming with threats and opportunities, that could make or break the new automated business models most organizations are migrating towards.

9. Do we need more awareness, resources and expertise to tackle these threats?

Staff training and the recruitment of experts is a key consideration in cyber security. Staff will need to understand the way data is classified and the way each type is handled when dealing with colleagues and outsiders. One crucial issue is a whistleblowing system where staff can report any concerns with the way information is being used or weaknesses that they have observed. Staff should also be trained about the dangers of social media and criminals who use social engineering, including 'chance meetings' at social events to 'get inside' employees and obtain what should be confidential data such as their passwords. Telling social contacts about work responsibilities is a sure way to attract the attention of criminal gangs. There are huge risks associated with USB drives and laptops that are taken off site and which contain loads of sensitive data. In future, street robbers may leave the victims cash, wallet, cards and valuables and simply steal any phone sim cards and USB sticks to maximize their gain from the personal data, emails, automated on-click passwords and browsing history as cyber crime pays much more than old fashioned theft. Poor patch and anti-virus update management may mean some business systems become more vulnerable to attack.

Cyber Security (Page 6 of 6)

10. Where do we stand in terms of our competitors in the way we are meeting these new challenges?

To stay ahead an organization needs to keep up and then move away from the competition. Since comparison web sites make it more and more difficult to sell something based solely on the lowest price, some consumers are looking for the value-add when choosing their supplier. And some of this value add may sit within the way a company protects its customers' data, even if they do not offer the lowest price. In the past, it was argued that people needed to pass two out of three tests to access and use an on-line service:

- Something one knows, such as a password or answer to a security question.
- Something one has, such as a passport, physical token or an identity card.
- Something one is, such as biometric data, like a fingerprint, iris or face scan.

It may be the case that good organizations find a way of using all three measures to ensure the person who is authorized for the system should be authorized. Moving from access controls, one challenge is to merge IT security into a much wider IT Governance policy that is a key part of the overall corporate governance arrangements which lie at the feet of the board of directors. We can summarise the questions that the board may want to ask when considering cyber security:

1. What type of risks are coming on line?
2. How do these risks materialize?
3. What are management's legal obligations?
4. What do these risks entail in terms of impact on operations and the likelihood that they will materialize?
5. What does the IT security strategy currently do about these risks?
6. What does management do when there is an adverse event?
7. How can management stay on top of things?
8. Is the entire workforce mobilized against these new and emerging threats?
9. Does management need more awareness, resources and expertise to tackle these threats?
10. Where does management stand in terms of our competitors in the way they are meeting these new challenges?

Fraud Risk Management

Before we go to the next part, let me give you a concluding remark.

A threat becomes a risk when you can define it and make an effort to deal with it. You should visualize the threat, arm yourself and take aim.

Your Tutorial

5. RED FLAGS

A Question

You run a small purchasing section and your deputy, Paul's job is to visit key suppliers to negotiate discounts for the company. He never takes time off and has refused promotion to more senior roles. He mentions that he may need time off to visit his mother who is ill. You remind him that he has several planned visits but tell him Sue, another team member, can cover these. Paul immediately becomes upset and says he will not need to take time off after all. Would you be concerned about this situation?

1. Cannot see a problem at all.
2. There is not much you can do about touchy staff.
3. You should be very concerned about this.

Would you chose 1, 2 or 3 as the most appropriate response?
The correct answer is on the next page.

An Answer

You may want to talk to your own boss about why Paul does not want cover for his job as procurement is an area ripe for fraud and corruption. People involved in fraud often become stressed through a mix of guilt and fear. They can become anxious and very sensitive about answering questions concerning the way they work. On the other hand, it could simply be that Paul is worried about his job if someone else covers for him.

?

1 ✗ Cannot see a problem at all.

2 ✗ There is not much you can do about touchy staff.

3 ✓ You should be very concerned about this.

Can You Spot The Fraudster?

Let's say someone is defrauding your company.

Study the images and notes carefully.

Which person is most likely to be THE FRAUDSTER.

Jason works in procurement and approves contracts. He was appointed three years ago.

Julie has been part of the Chief Executive's support team for more than ten years.

Susie works in the payments team and will be going on maternity leave next month.

Steve joined as a temporary contractor providing technical IT assistance last week.

Can You Spot The Fraudster?

There are some jobs and some positions that hold more risk in terms of employee fraud but in truth, all choices are wrong. Trusted, long serving colleagues can surprise everyone by getting involved in underhand practices.

In reality, it is not really possible to tell whether someone is defrauding your organization unless there are clues that suggest not all is well.

We will be dealing with these indicators next.

Jason works in procurement and approves contracts. He was appointed three years ago.

Julie has been part of the Chief Executive's support team for more than ten years.

Susie works in the payments team and will be going on maternity leave next month.

Steve joined as a temporary contractor providing technical IT assistance last week.

Responding to Suspicions

Your job is to be aware of signs that not all is well and respond to them.

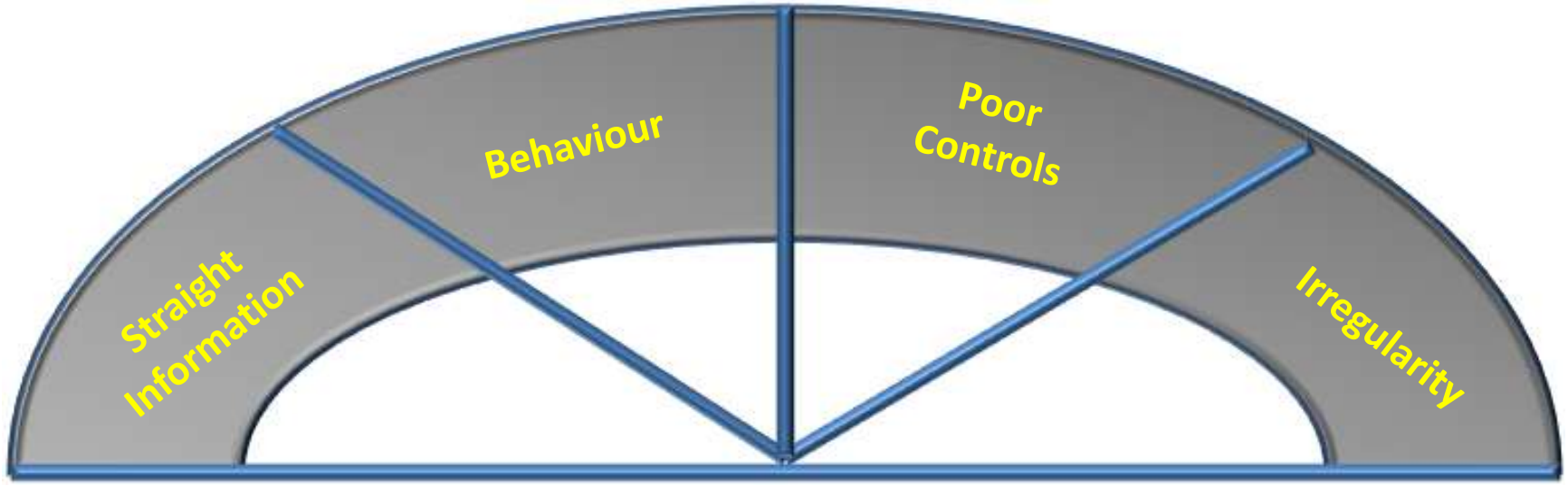
- What are my suspicions?
- Which laws and/or procedures are affected?
- What information do I have so far?
- Who should I talk to?

Some Red Flags

There are some so called 'Red Flags' that appear in organizations and teams that could suggest fraud is happening.

One simple approach is to classifying them in four ways.

If you want to explore this idea of suspect behaviour, there is a short note on the next page that you can read or simply skim through.



Straight Information
At times, information comes directly to light that on careful consideration should indicate something is wrong.

Poor Controls
Individuals will not normally be able to commit fraud without a lapse in the systems of internal control. Where there are specific gaps in controls there can be a climate that does not help contain fraud.

Behaviour
These indicators relate to the way people at work behave, like frequent absences, being in debt (or having loads of spare cash) or being really protective about their area of work.

Irregularity
Unlike straight information, there are other indicators of fraud that are circumstantial in nature. Many are due to simple error but others result from the intentional manipulation of records that results in trends inconsistent with business activity.

Red Flag and Behaviour

Behavioural Issues

These indicators relate to the way people at work behave and can include:

* Regular Absences: This could indicate a personal problem.

* In Debt: Known to have low funds and lots of debt. A motive for some fraudsters is solving a severe financial problem which means a person with mounting debts could have a strong motivation to commit fraud at work.

* Protective Behaviour: Where the person does not take their holidays, works long hours, is hardly ever sick and keeps their working papers very close to hand there is little chance of anyone intruding into their work. If files are being doctored - the person may be diverting refunds on say accrued loan interest on the early loan repayments from clients and paying these refunds into a private bank account. This scam could go on for a while as long as no one checks the refund files and the customer may not realise they are due a refund. One indicator is for the employee to become very defensive and aggressive, again to ward off any unwanted inquiries.

* Addictive Behaviour: Someone who drinks excessively, takes illegal drugs, or gambles will have to support an addictive and possibly expensive habit. Addictive habits take money to support and these activities may be deemed by some as anti-social. A loner may be less able to share personal problems and some argue that fraud results from having a financial problem that cannot be shared, hence the person resorts to illegality.

* Strange Behaviour: Where the person is struggling with guilt it may affect their persona. In addition, a fraudster may become really upset when someone else tries to deal with a large supplier who is normally only dealt with by them. Moreover, the individual may also become agitated when asked to explain an odd transaction.

* Inappropriate Wealth: This indicator is pretty obvious. If an employee's income less their expenditure results in a lifestyle and assets that do not add up, there is the possibility of unexplained income from illegal sources. Not the only possibility but just one explanation.

Report to The Nations

A quote for you from the ACFE.

We'll have look at a short case study next.

Most fraudsters do not undertake their scheme expecting they will be caught. When people choose to engage in occupational fraud, they typically know that they are risking their careers, reputation and freedom by engaging in such misconduct. Therefore, increasing the likelihood that a scheme will be detected is a pillar of fraud prevention.

Jane worked as the office assistant in a local authority young homeless people's Centre. The Centre depended on a great deal of cash transactions to operate.

The youngsters would be given cash allowances by support workers who also paid for many essential items from their own pocket and then claimed the cash back on a daily basis.

One of Jane's tasks was to process cash payments to support staff who would submit their claims and vouchers after getting them signed-off by a team leader.

Jane's manager would check the claims and vouchers each week. The documents would be double checked by the finance department who issued regular cash funds to Jane.

LIVE CASH CLAIM FORM	**REF**
EXPENDITURE	**£**
Dinner costs	55
Allowances Client C1126	130
New kettle	23
TOTAL	**208**
……	……
SUPPORT WORKER	DATE
……	……
TEAM LEADER	DATE

(Pease attach vouchers)

Do you think this is a secure system?

LIVE CASH CLAIM FORM	**REF**
EXPENDITURE	**£**
Dinner costs	55
Allowances Client C1126	130
New kettle	23
TOTAL	**208**
……	……
SUPPORT WORKER	DATE
……	…….
TEAM LEADER	DATE

(Pease attach vouchers)

A Short Case study

Many simple systems can be abused by people who know the system and use their knowledge to hide wrongdoings.

Jane would insert an additional line in some of the claims, change the total and make up a fake voucher – and keep the difference.

The records examined by Jane's boss and the finance staff appeared to be okay.

Let's do one more case study next.

LIVE CASH CLAIM FORM	**REF**
EXPENDITURE	**£**
Dinner costs	55
Allowances Client C1126	130
New kettle	23
Travel (Petrol)	30
TOTAL	**238**
……	……
SUPPORT WORKER	DATE
……	……
TEAM LEADER	DATE

(Pease attach vouchers)

Another Short Case study

Have a look at this table of staff commission for departments A to D and make a note of anything that may need to be examined in more detail.

SALES STAFF COMMISSION £,000

	LAST PERIOD	THIS PERIOD	INCREASE IN SALES THIS PERIOD %
Dept. A	100	80	-10%
Dept. B	210	300	+5%
Dept. C	150	160	+5%
Dept. D	110	110	0%

Another Short Case study

First do a bit of work. Calculate the difference between the two periods.

SALES STAFF COMMISSION £,000

	LAST PERIOD	THIS PERIOD	DIFF	INCREASE IN SALES THIS PERIOD %
Dept. A	100	80	-20	-10%
Dept. B	210	300	+90	+5%
Dept. C	150	160	+10	+5%
Dept. D	110	110	0	0%

Another Short Case study

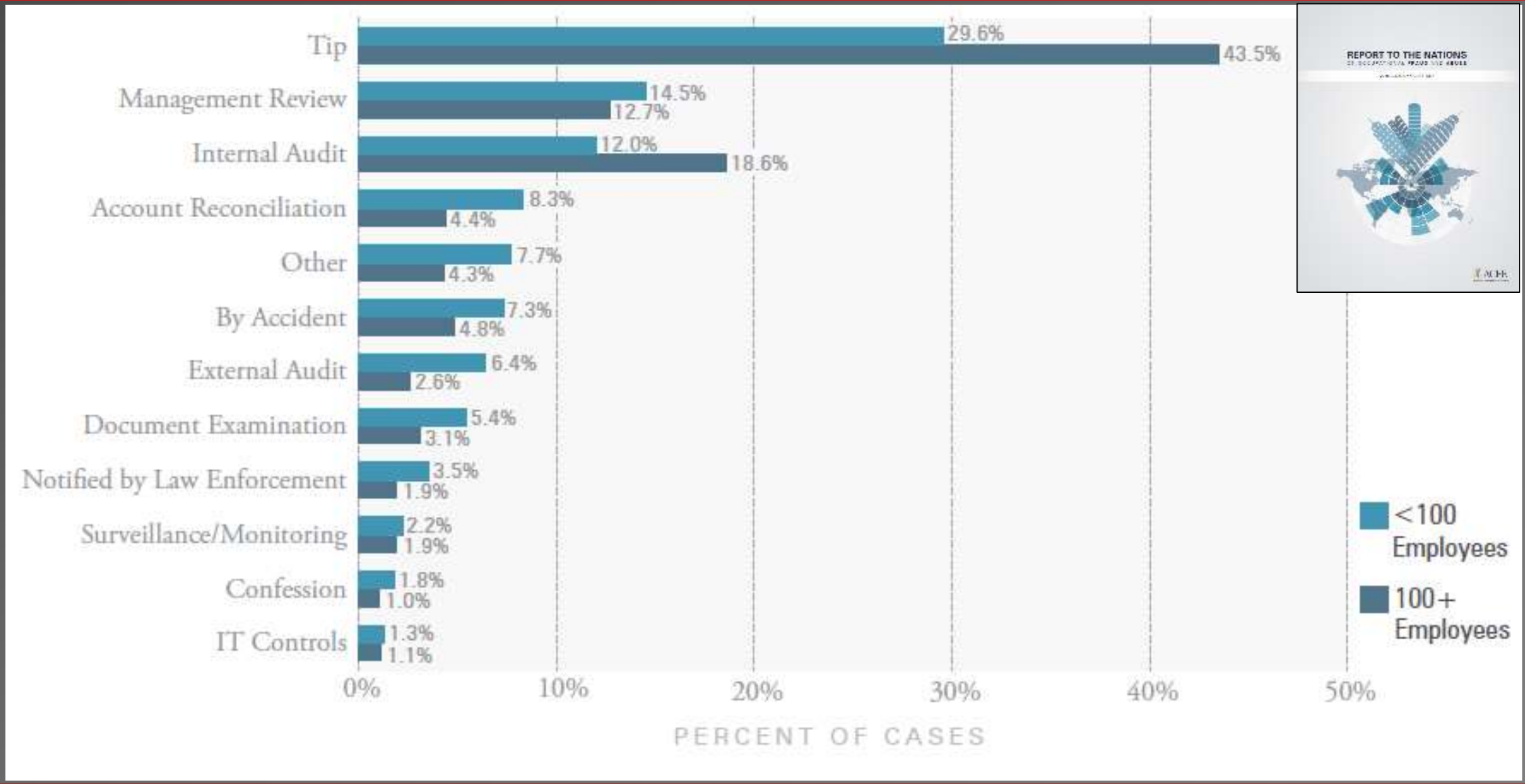
It may be an idea to investigate the increase in commission for Department B because it is out of step with the increase in sales. It could be due to error, or misadministration.

It is when all sensible explanations have been explored that we eventually come to the possibility of fraud.

SALES STAFF COMMISSION £,000

	LAST PERIOD	THIS PERIOD	DIFF	INCREASE IN SALES THIS PERIOD %
Dept. A	100	80	-20	-10%
Dept. B	210	300	+90	+5%
Dept. C	150	160	+10	+5%
Dept. D	110	110	0	0%

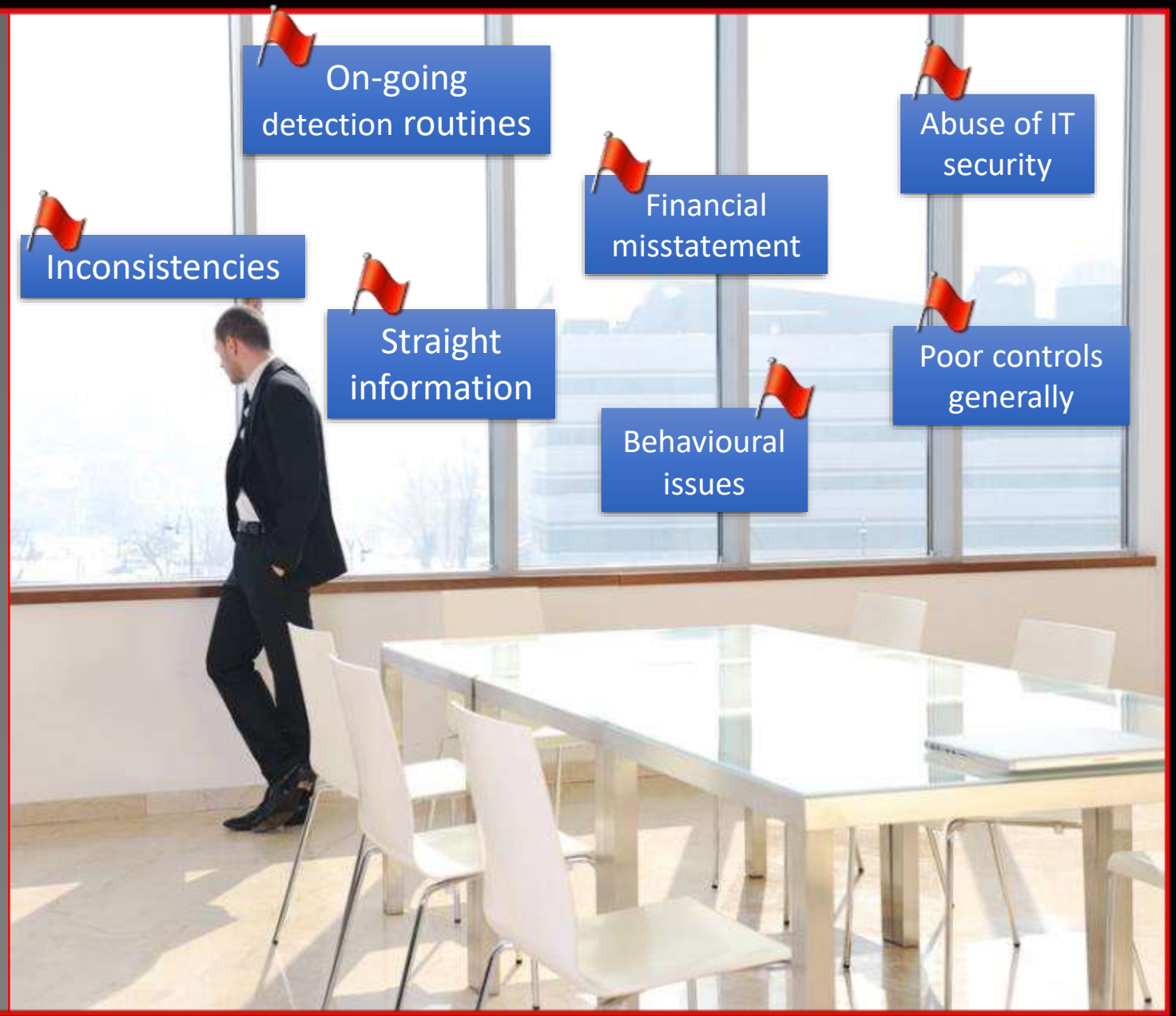
According to the ACFE just over half the tips came from employees. Customers and vendors were also high on the list.



Some Red Flags

Let's look deeper into clues that all may not be well in many organizations.

Here are some of them and if you want a bit more information have a look at the next page.



Some Red Flags

Inconsistencies

- Trends inconsistent with activity
- Reconciliation differences
- Strange contract figures
- Lost assets
- Fictitious items

On-going detection routines

Specialist software is used by some organizations to monitor, flag up and identify suspicious activity by staff, although not all organizations use such programmes proactively.

Straight information

- Complaints from suppliers, partners and customers
- 'I owe yous' (IOUs)
- Information from whistleblowers

Financial misstatement

- Performance pay and huge bonuses
- Share price pressures
- High tax bills
- Poor board oversight
- Financial problems

Behavioural issues

- Regular absences
- Known to have low funds and lots of debt
- Protective behaviour
- Addictive behaviour
- Strange behaviour
- Inappropriate wealth
- New staff resigning quickly

Poor controls generally

- A lack of segregation of duties
- Systems override
- Poor state of controls awareness
- Poor audit, accountability and board oversight
- No controls over HR processes
- Large amounts of staff overtime
- High staff turnover
- Conflicts of interest
- Flat organizational structures
- Poor accounting controls

Abuse of IT security

- Poor segregation of duties
- Poor programme control
- Poor exception reports
- Poor virus detection
- System activities not traceable
- Password unchanged and uncontrolled
- Output not verified
- Lack of proper sanctions

The Reality of Speaking Up

Whistleblowing is a great way of finding out about wrongdoing including fraud at work, but it not always easy.

Where there is a culture of looking the other way, people become very scared of telling all.

In October 2012 allegations about sexual abuse of young girls emerged regarding the late British TV personality Jimmy Savile. It seems many people knew about these problems but because he was so famous he got away with it.

Why Keep Quiet?

We know we must report suspicions of wrongdoing.

But there are many reasons why this does not always happen.

Let's whiz through a short case study on whistleblowing next.

I'm really worried about any reprisals.

My boss is gonna look stupid for not spotting it.

Not really sure how to report my suspicions.

There must be some excuse for this odd behaviour.

I don't want to get involved in a fuss that could mess up my career.

I just feel sorry for my colleague, even if he's up to no good.

Your Whistleblowing Case Study

After a restless night Peter, a 68 year old retired engineer, woke up Sunday morning and experienced severe headaches and dizziness, and took some painkillers. He continued to feel unwell and phoned a taxi which took him to Accident and Emergency (A&E) of his local public hospital arriving at just after 12pm. He gave his details to the reception staff who asked him to wait for a nurse to assess him. He waited patiently and dozed off a few times.

At around 6pm he saw a nurse who contacted his son, David (Peter's wife died a year ago) and took him to an assessment unit. A junior doctor diagnosed him and admitted him to the stroke unit for further tests. He spent three days in hospital and was released to his son's care with slight paralysis of his upper left body.

Peter was traumatized by the experience and told his son that his memory of the day was very hazy but he felt he had waited all afternoon before he was seen by medical staff.

Your Whistleblowing Case Study

David studied the hospital's web site and discovered that they boasted about exceeding government targets by treating all emergency patients within 4 hours of their arrival. He e-mailed a formal complaint claiming that the target times had been sorely missed.

He received a response from the Complaints Team the next day, which stated that his father had been seen and assessed within two hours and there was no 'undue delay' involved in dealing with him. David then contacted the taxi company his father had used to get to the hospital and found out that the driver had recorded the trip as 'early afternoon customer drop off'.

WHAT WOULD YOU DO?

Your Whistleblowing Case Study

David contacted the Complaints Team with this new information but was told that the case had now been closed. In desperation, he called Accident and Emergency and spoke to Anita, an admin support officer who worked for the Accident and Emergency Team.

He told her about his complaint and that he was not satisfied with the response.

Your Whistleblowing Case Study

Anita was surprised to receive the phone call from David and had the impression that he was very upset by his father's condition and had probably got his facts wrong. She promised to look into the matter and get back to him.

WHAT WOULD YOU DO?

Your Whistleblowing Case Study

Anita checked the admissions log and treatment data for Sunday and it seemed that Peter was seen by nurse Atkins after 2 hours of his arrival and was then admitted later on in the day for a series of suspected strokes.

He was then given the standard procedure for stroke victims and after intensive treatment, discharged three days later. She sent an email to David confirming that all timings stated in the response to his complaint were correct and that he would have to view the hospital web site for the procedure for disputing the way his complaint was handled, in the event that he wanted to take the matter further.

Anita bumped into Nurse Atkins later that day and mentioned that she had spoken to Peter's son.

Atkins remembered Peter and said that she came on shift at around 5pm and the A&E receptionist told her to have a look at him because he had been there since lunchtime. She had seen him at 6pm and called his son, David as he had to be admitted to the stroke unit.

WHAT WOULD YOU DO?

Anita spoke to her manager and explained that there was a discrepancy between the information on the admissions system and the details she had been given by the patient's son and nurse Atkins.

Her manager, Tom Dowdry, was very busy and said to her, 'Look - Complaints have dealt with the matter and we do not get involved in this sort of things. Just leave it alone and let's concentrate on what we are paid to do.'

Your Whistleblowing Case Study

Anita checked the 'Speaking Out' staff policy guidance and found a note that suggested staff who felt systems were recording incorrect information should relay their concerns to the appropriate Head of Service.

Anita asked to see June Brown, the Head of Emergency Care who told her to meet outside the conference room as she was due to attend a meeting there. Anita explained her worries about the way Peter's case was being recorded and the Complaints Team's investigation. June told Anita to leave it with her and she would look into it.

WHAT WOULD YOU DO?

Your Whistleblowing Case Study

Anita decided to a-mail June Brown as follows:

Many thanks for looking into the Peter Durrant case following our meeting earlier today. I would like to contact his son, David, and explain that we are reviewing the case further. Please let me know if I should provide any further information at this stage.

Later that day June Brown asked Anita to come to her office and told her not to contact David and to stop looking into the admissions system as it was not her responsibility.

June explained that the Complaints Team had considered this case in some detail and it was not in the best interests of the hospital to re-open the matter. She made it clear that Anita had already disobeyed her line manager, Tom, and if she did any further work on the case she may end up being disciplined for failing to follow clear management instructions.

WHAT WOULD YOU DO?

Your Whistleblowing Case Study

The following day David called Anita and said he had finally spoken to the taxi driver who had taken his father to the hospital who confirms he arrived at around 12pm. He gave Anita the driver's contact details and asked her to see what she could do.

Anita checked a few more cases and there appeared to be a pattern where many patients were logged into the system and their arrival times were amended. Anita accessed the 'amends log' which showed that each of these times were being changed to a later time. When she logged on to the system after lunch she received a message that her access to amendment reports had been withdrawn.

Your Whistleblowing Case Study

Anita felt distressed. Tom, her manager, explained that access for team members had been reviewed and some of her access rights had been removed because she was getting involved in things outside her responsibility. Tom was quite rude and suggested she may want to seek a transfer to a different team if she did not like the way they worked here. Anita felt that some of the other team members were avoiding her apart from her close friend Sarah who told her to keep her head down and it should blow over.

Anita contacted everyone she trusted and explained her predicament, making sure she used her own, and not her work phone. She spoke to her parents, her union, her friends and her cousin who worked as a doctor at a different hospital.

She contacted a well known charity that assisted whistleblowers and met with her union representative who arranged a meeting with the hospital's Chief Executive, who had only been in post for a few months.

Your Whistleblowing Case Study

The newly appointed Chief Executive ordered a full investigation into manipulation of admissions and waiting times at Accident and Emergency. The Director of Emergency Care was suspended and Anita's manager, Tom was severely reprimanded. Anita never recovered her good relationship with her team as they had been told she was a trouble maker and could not be trusted.

She left her job at the hospital and got a job as a senior business support manager at a local health centre. Her actions meant A&E was restructured to ensure delays were minimized and the practice of changing arrival times ceased.

Patients such as Peter may now have a much better chance of receiving early interventions in future and Anita's parents told her how proud they were, knowing that she played a role in securing these improvements.

Speaking Up

Speaking up when everyone around you is keeping their silence is so hard to do.

You may need to walk against the tide.

And it is only by holding on to a belief that you are doing the right thing that will help you stay on track.

The key lesson from to our case study is to seek the help of others.

The next page contains a few notes on whistleblowing resources.

Whistleblowing Facilities

Reporting illegal activities should be actively encouraged throughout the organization. Exit interviews for all staff may also be used to elicit information from people who may have no reason not to act in good faith.

1. The facility should be administered by professional staff and operate on a 24 hour basis and not be located in the organization's offices.

2. It is often difficult to use the facility and if the corporate culture does not support transparency at work, whistleblowing may be discouraged.

3. Each employee has a duty to make known any concerns they have at work and this should not really be optional. Moreover, there is legal protection where whistleblowing has been used in the correct manner.

4. It is important that the facility is used properly, which means it should not be exploited or used inappropriately. The line manager is normally the first point of call and there are only a few occasions where disclosure to people outside the organization is condoned.

5. All senior people in the organization should be open to concerns from their staff and understand the need to clear up problems at an early stage.

6. There is a need for employees to be loyal to their employers and to protect their interests, which is why it is important to use the set whistleblowing procedures.

The Public Interest Disclosure Act 1998 applies to England, Scotland and Wales and disclosures relating to crimes, breaches of legal obligations, miscarriage of justice, dangers to health and safety or the environment and concealing information relating to these items. In the US, the SEC has awarded more that $175 million to whistleblowers since the inception of their program in 2011 on federal security law violations.

Red Flags

Before we go to the next part, let me give you a concluding remark.

Don't be nosy, don't be negative but do keep an eye out for anything that does not make sense. Or anything that points to wrongdoing – and act.

Your Tutorial

6. FRAUD RESPONSE

1. Understanding Fraud Risk
2. Defining Roles
3. Your PRS Context
4. Fraud Risk Management
5. Red Flags
6. Fraud Response
7. Conduct & Controls
8. Your Dynamic Role

Business Fraud Risk Management

PROGRESS MARKER 68 %

A Question

You are the team leader for a small team processing refunds to customers. You suspect that a new team member is fraudulently diverting some payments to a special account he has set up. How would you respond regarding this possible fraud?

Would you chose 1, 2 or 3 as the most appropriate response? The correct answer is on the next page.

?

1. Would you carry out discreet enquiries?
2. Would you confront the suspect?
3. Would you just report your concerns?

An Answer

You will need to report your concerns immediately to the appropriate party named in your anti-fraud policy.

But do not carry out your own investigation.

?

1 ✗ Would you carry out discreet enquiries?

2 ✗ Would you confront the suspect?

3 ✓ Would you just report your concerns?

Fraud Response Policy

We have dealt with many of the items on a typical anti-fraud policy and now we need to address the aims of the fraud response plan that should swing into action when an actual fraud is discovered.

- Prevent loss and maximise recovery of losses
- Identify the fraudster
- Identify lessons learnt and act on them
- Publicise details of prosecutions
- Minimise fraud by rapid action
- Minimise adverse publicity
- Reduce adverse impact on the business
- Correct weaknesses in internal controls

Responding to Allegations

Your job is to report your suspicions and not become some sort of secret agent.

Have a look at your fraud response plan at work and follow it to the letter.

If you come across a fraud at work it will need to be examined by experts who will need to gather the evidence with great care.

The next page contains a note on fraud investigations just in case you want to understand how they work.

Fraud Investigations - Evidence Gathering

Fraud investigations are primarily about gathering compelling evidence that is enough to support a criminal conviction:

- The evidence should either engender a guilty plea from the defendant, or be able to support a criminal prosecution. Any confession by the suspect must be entirely voluntary.
- The evidence must comply with various legal rules regarding admissibility. So if it is misleading, prejudicial or wastes the time of the courts or is just mere speculation then it may not be legally admissible. For example, claims of unreasonable entrapment should be avoided. This is where the crime would not have arisen otherwise than through efforts to tempt the person.
- The defendant may prepare a case that seeks to refute or discredit the evidence presented by the prosecution. In fact, defence will have sight of the evidence used by prosecution and disclosure of certain basic items may be provided to defence even if they are not asked for. This is to ensure defence understands what evidence is held and is in a position to request copies where required. At the start of an investigation, if an attorney is employed then the material will be confidential under client-attorney privilege, at least for a while. If the evidence is given to a third party this privilege may be lost.
- It may be in the interests of the defendant to ensure the evidence that supports the prosecution case is not readily available or forthcoming. This also applies to potential witnesses, and documents that were in the possession of the defendant. It may be necessary to agree disclosure and admissibility with defence beforehand and save time in courtroom debates.
- The standard of proof for criminal cases is such that it can convince a jury that there is no reasonable doubt that the defendant is guilty.
- Evidence costs money to acquire, maintain and present. It also takes time and the value from the evidence and its impact on the case has to be weighed up against the cost of adding it to the case for the prosecution.
- The onus is on the investigating team to ensure the evidence is sufficient, relevant and reliable. If the evidence is simply someone's opinion, unless that person is an expert witness, it may get disregarded.
- Hearsay relates to evidence that has been told to a third party because the prime witness is not present to give the evidence and so cannot be cross examined by defence. As such, it is generally disregarded.
- If there is any break in the chain of evidence that links the crime with the defendant, then the evidence may be deemed unreliable and disregarded by the courts. The evidence itself may be sound but the way it as obtained, stored and presented may impair its reliability.
- If the rights of the defendant are violated in the process of securing the necessary evidence, this evidence may well have to be abandoned.

The Nature of Evidence

There are different types and categories of evidence that will be gathered during a fraud investigation.

One simple classification is shown here. Note that really good evidence is direct evidence that has been corroborated by another reliable source.

One reason trained investigators deal with fraud work is that evidence has be admissible to be used to support a criminal prosecution. It is crucial that you don't get involved in investigating fraud as you may mess up the strict evidential requirements required by the courts.

Some of the reasons you should report suspected fraud and not conduct your own investigation are set out on the next page.

TYPES OF EVIDENCE

TERM	EVIDENCE
1. Direct Evidence	This is straightforward evidence that will establish the truth regarding the facts in question.
2. Circumstantial Evidence	This is indirect material that establishes some degree of likelihood of the facts being established.
3. Hearsay	This is an account of something that was said to the person providing the evidence.
4. Corroborated	This is where one source of evidence confirms another source of evidence.
5. Authenticated	This is where it is possible to establish that the evidence is genuine.
6. Expert Opinion	This is the professional opinion from a specialist on the topic in question.

Reasons Not to Investigate

Insurance claims for employee fidelity cover may become void if losses caused by the fraud are compounded by the actions of company representatives.

An over enthusiastic employee may confront the suspect and cause the individual to sue the company for false accusation and even false arrest.

An employee may investigate the alleged fraud and inadvertently breach the corporate procedures on conducting such investigations.

The chain of evidence may be broken.

Cases that should be properly put before the police may be referred too late to the authorities.

The workforce may feel humiliated and de-motivated if people are implicated by association.

Mistakes could be made at the start of the investigation that are irretrievable.

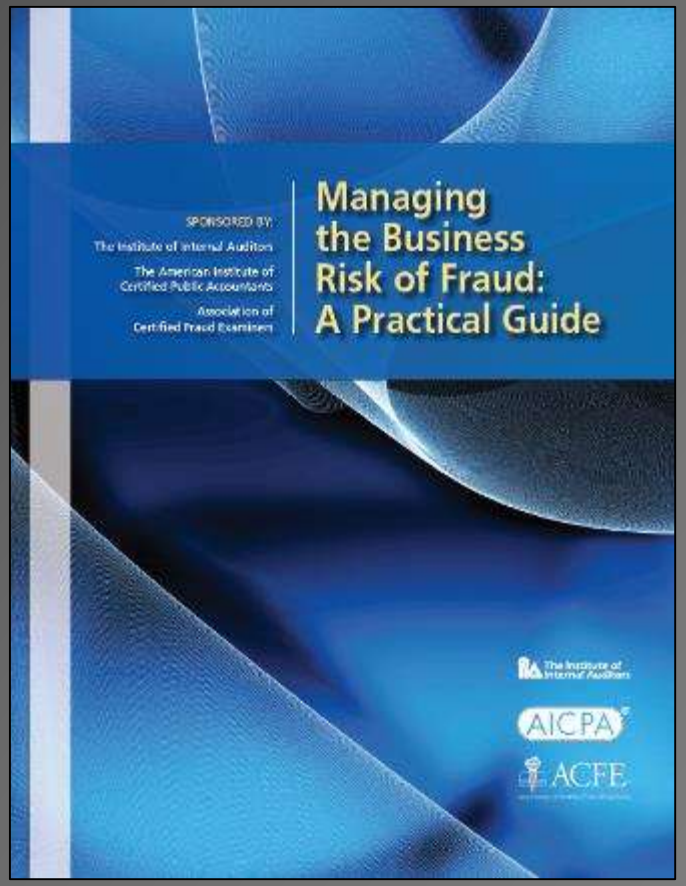
The suspect may be given a promise not to prosecute which may not be appropriate.

The suspect may be alerted.

The constitutional rights of the suspect may be infringed.

Managing the Business Risk of Fraud

A quote for you.



The board and the organization should establish a process to evaluate allegations. Individuals assigned to investigations should have the necessary authority and skills to evaluate the allegation and determine the appropriate course of action.

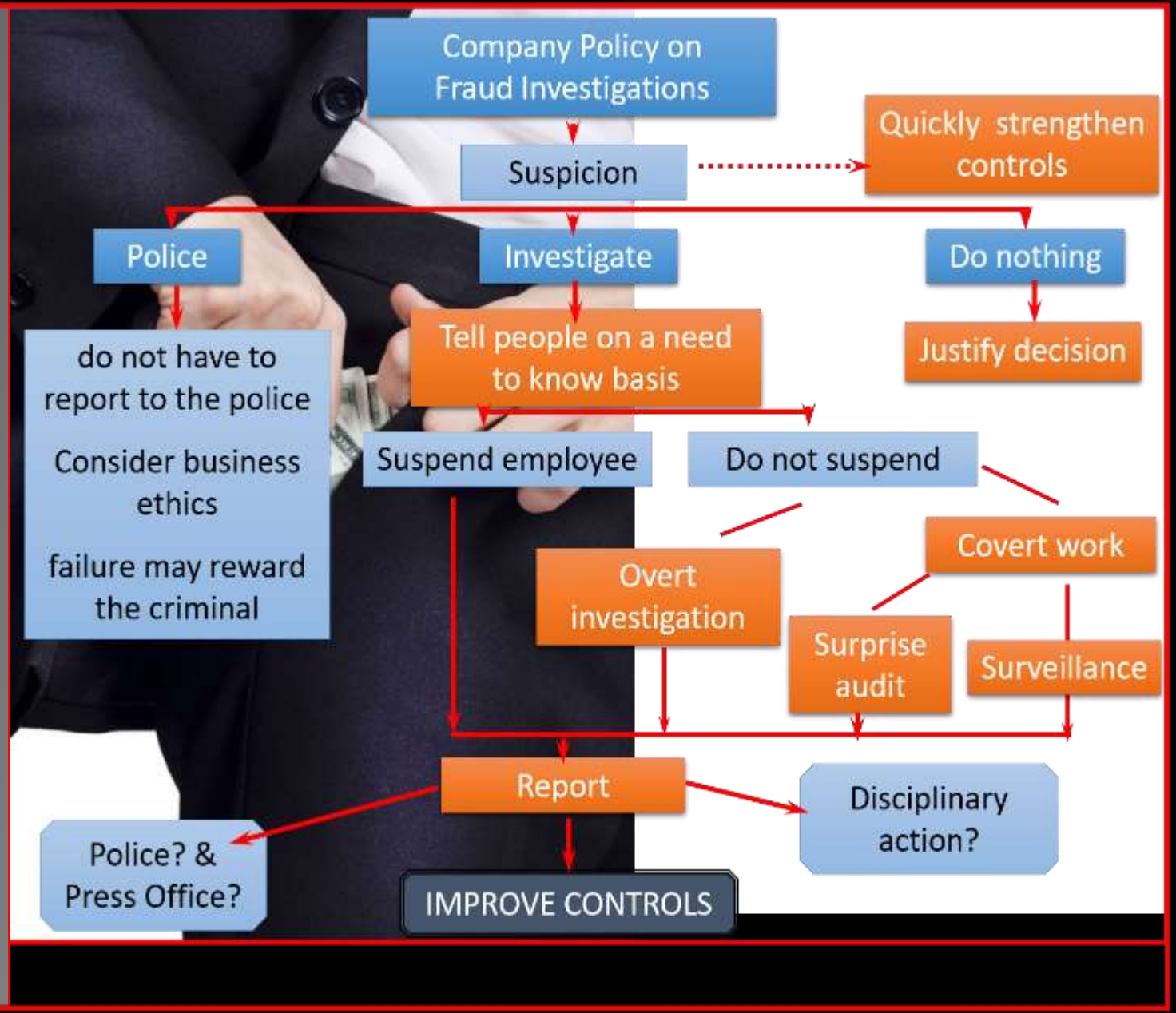
Fraud Investigations

We have developed a simple Template to cover the way a corporate policy and procedure dealing with allegations and fraud investigations may be structured.

Fraud awareness is not about conducting investigations but if you want to read about some of the basics you will find a short note on the next page. There are several things you will need to consider when confronted by a fraud:

- Referring the case to the criminal justice agencies.
- Disciplining the employee.
- Claiming against the relevant insurance policy.
- Launching a civil case for recoveries of monies lost.

A final note on investigations follows.



Fraud Investigations

The main investigation will be carried out with a view to securing the available evidence and discovering the truth. The employee in question may be suspended if the evidence would otherwise be at risk. Or, the investigation may start out as covert to secure live evidence if required:

- **Securing evidence:** This is a crucial stage as an investigation is about uncovering the truth and securing evidence that is sufficient, reliable and convincing enough to support subsequent charges using the rigorous standards of the criminal justice system. Tainted evidence is evidence that has lost its integrity, infringes the rights of the suspect or simply breaches the rules of evidence gathering set by criminal law; which means it might get thrown out of court.
- **Interviewing:** Witnesses, colleagues managers and others will be interviewed to secure evidence that supports the investigation by proving or disproving the allegations.
- **Confidentiality and media contact:** During the course of the investigation regard will be had to confidentiality and the way the media will be informed about events. It is best to use one channel of communication, say the press office so as to control the proceedings and guard against defamation and excessive damage to the corporate reputation.
- **Action options:** The investigation will result in a report that will give direction as to possible criminal proceedings and staff disciplinaries for gross misconduct. The disciplinary may well be based around breach of procedure and possible dismissal at an early stage where there is sufficient evidence regarding the conduct of the employee. Meanwhile, the police case will focus on criminal charges and a conviction, which may take time to conclude.
- **Recovery:** Throughout the investigation the question of recovery and damage limitation will be assessed, although offers for the return of funds by the suspect will have to be discussed with the company lawyers.
- **Control fixes:** While the above investigation is being progressed, management should be involved in fixing weakness in internal controls as part of the ongoing fraud risk management process.

Fraud Response

Before we go to the next part, let me give you a concluding remark.

If an allegation of fraud is made or a fraud breaks out, act responsibility. Go straight to your fraud response plan and stick to it.

Your Tutorial

7. CONDUCT & CONTROLS

A Question

You are the new manager of a charity shop which employs a team of low paid retail staff and some volunteers. On your first day your assistant, Sheila, says that the old manager used to let staff take goods home and put a few pennies into the cash till. She asks whether you have any problems about continuing this simple arrangement.

Would you chose 1, 2 or 3 as the most appropriate response? The correct answer is on the next page.

?

1. Not really - so long as staff do not get too carried away.
2. Not really - it's easier to just let staff take home the clothes and not worry about any payment.
3. None of the above.

An Answer

You really need a proper system for sales to staff and volunteers that cannot be abused.

Perhaps they could be given a set staff discount and maybe a maximum number of items they can take home each week.

?

1 ✗ Not really - so long as staff do not get too carried away.

2 ✗ Not really - it's easier to just let staff take home the clothes and not worry about any payment.

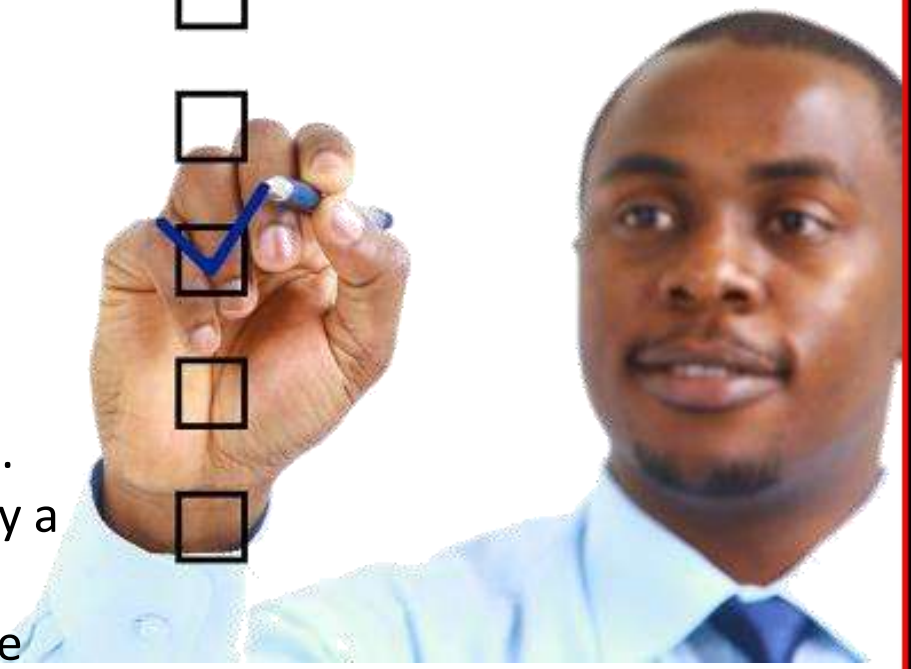
3 ✓ None of the above.

Employee Discipline

It is essential that you stick to the disciplinary procedure when dealing with misconduct cases.

And any investigation needs to be carried out in a fair and balanced manner.

- The employee must have breached the disciplinary code of conduct.
- He or she should have been made aware of the potential consequences of the breach.
- The circumstances should have be formally investigated.
- The findings should be based on sufficient, reliable evidence and the employee should have been given the right to explain their version of events.
- The employee may be accompanied by a colleague or union representative.
- A formal disciplinary hearing should be held to consider the facts and make a decision.



- A facility to appeal the decision made should be in place.

The above should be based on a reasonable and transparent process that coincides with best practice and any codes that cover the organization in question.

Employee Discipline

Corporate policies should make several things clear to the employees.

It is essential that you stick to your disciplinary procedure when dealing with misconduct.

And your fraud team's investigation should be both fair and thorough.

Employees shall have no expectation of privacy when using telephones, computers, mobiles, radios or other communications provided by the employer. Lockers, desks, company phones, computers and vehicles may be searched with the employee's consent, with reasonable notice or with a valid search warrant and in the presence of a witness. Such searches will only be conducted where there is reasonable suspicion of misconduct or under a search warrant.

Disciplinary Panel

If the disciplinary process swings into action, a panel will need to be convened to consider the charges and whether they are proven or not.

- The disciplinary panel may consist of senior managers and an officer from HR.
- The panel will hear the charges presented by an independent manager based on the evidence gathered during the internal investigation.
- The employee (or their representative) will present their defence to these charges.
- Witnesses may be called by both sides and cross examined.
- The panel will reach a decision on whether the charges are proved or not based on the balance of probabilities, and recommend any appropriate sanctions.
- A senior director with advice from HR and Legal will decide whether to implement the panel's recommendation.
- The employee will have a right to appeal the decision to a new panel of senior managers.

Disciplinary Procedure

Decision

The panel will consider the evidence as presented, adjourn and then make a decision and recommend a suitable remedy such as not proven, dismissal, demotion, any formal sanctions and/or training and so on. The CEO (or representative) will consider the recommendations from the panel and endorse them if appropriate.

Proceedings

The disciplinary hearing shall follow a set procedure that provides a judicial response to the problem that is fair to both the employer and the employee, which may include some or all of the following stages in the following example:

1. The panel Introduces the hearing.
2. Each side makes an opening statement.
3. Presentation of the case by the employer including the examination of witnesses.
4. Presentation of the defence by the employer (or representative) including the examination of witnesses.
5. Each witness may be cross examined.
6. Questions from panel members seeking clarification from the employer and employee.
4. Both parties summarize their cases.
5. Adjournment.
6. Panel announces their decision at a later date.
7. Right to appeal with time limits made clear.

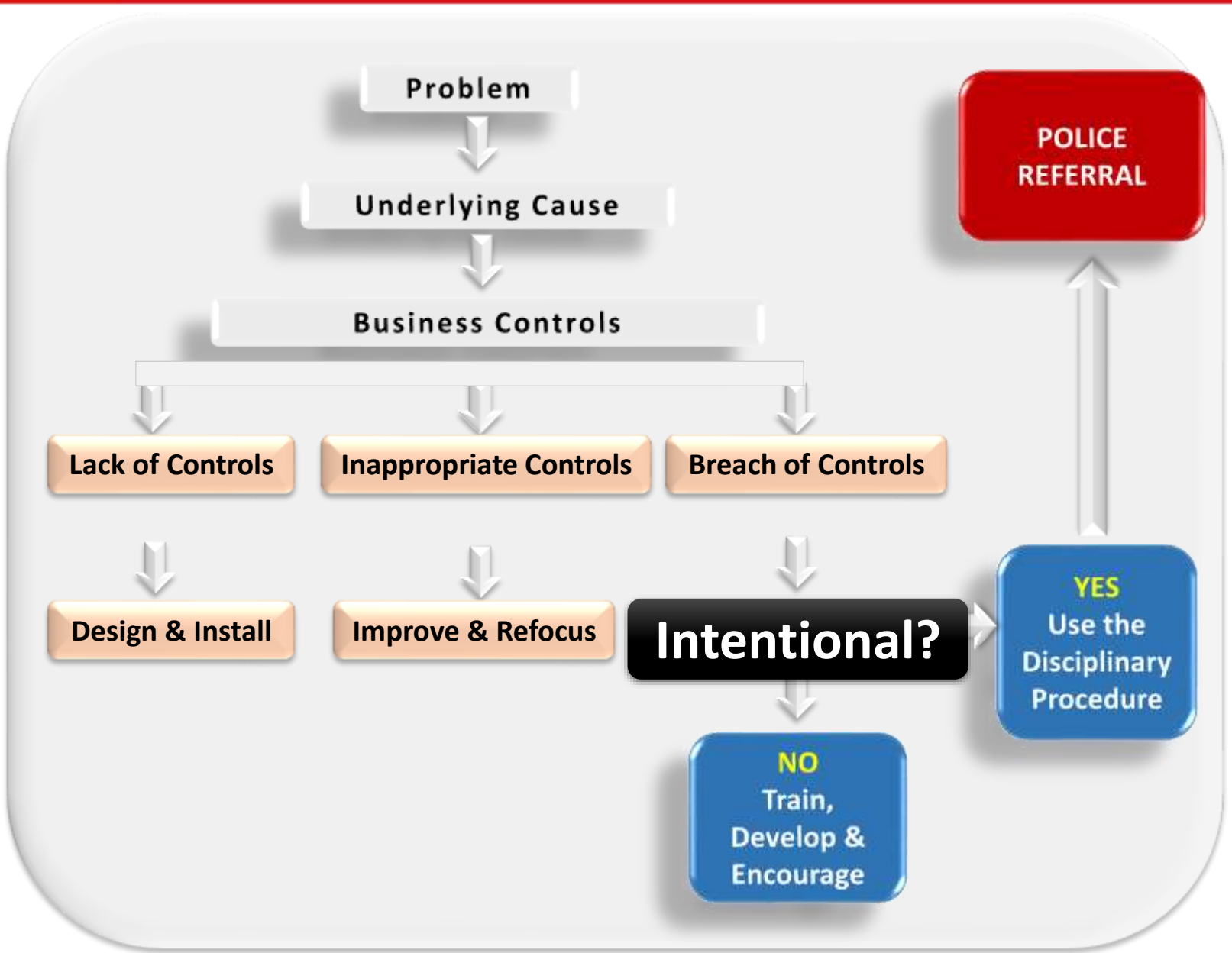
Appeals

The employee should have access to an appeals process if the disciplinary panel decides against them. The CEO, or representative, should hear the grounds for appeal and convene an independent appeals panel of senior managers to hear the appeal and decide whether there are grounds to change the decision of the original disciplinary panel. If an appeal is turned down, the employee may take their case to an employment tribunal and make a claim for unfair dismissal.

Disciplinary Process

The disciplinary procedure is in place to deal with misconduct. Where there is an intentional breach that relates to fraudulent behaviour then the matter should be referred to the police or whatever crime enforcement agency looks after employee fraud.

Employee fraud will always be a disciplinary offence that should result in dismissal if proven. This is why your disciplinary procedure should deal with the breach, unless the authorities ask that you take no action against the suspect.



Basic Controls

As you update your procedures, build in controls to ensure the risk of fraud, error and waste are adequately tackled.

Here are some basic control concepts that can be used to protect your business.

If you want more detail then have a look at the text on the next page.

- Supervisory Review
- ID Trails
- Verification
- Authorization
- Security
- Control Totals
- Information System Controls

Verification is an important concept, that depends on being able to check that something that should be there, is there. Stock-checks, and inventory reconciliations, inspections, asset checks and regular call-backs for assets used outside the office, means we have control over attractive and portable items. Cash-ups are a form of verification, where we ensure the money we should have taken actually exists and agrees with our records.

Authorization may be aimed at important transactions or decisions which have a high value/impact. The act of authorizing brings out other concepts; that of internal check and supervision, since a more senior person will get involved where necessary, to ensure significant transactions are correct and proper.

Security is another key control where we keep unauthorized persons away from valuable items, or information. Physical security is self-explanatory, whilst logical security is used by computerized systems, where say passwords and other devices are needed to access the various corporate and local databases.

ID Trails log the person who accesses a computerized system and that brings into play the concept of audit trails. Here, where possible, we trace who did what in any transaction. Physical access devices can also log individuals' activities. We can then get reports which show whether the patterns are regular, or if necessary, carry out investigations into someone's activities, if we later find problems to do with propriety.

Supervisory Review is another good control. We ask that managers and supervisors satisfy themselves that work is up to standard before it goes out. The way this is done is up to them but we can set standards in this respect. Organizations with poor staff disciplinary records normally have failings in this aspect of management. Either managers don't know what work is being done so can't review their people's work, or they just don't care.

Control Totals can be used to aggregate transactions and compare this with a separately held total to trace the movement of transactions through a system; to ensure that they're present and correct. Cash receipting incorporates this type of control.

Information System Controls cover general controls as well as controls over specific applications. These controls cover access security, software development, physical security arrangements, systems change controls, disaster recovery and contingency arrangements. Information system controls are all those arrangements that are there to maintain the integrity, availability and upgrades to the information processing capacity as well as the way information is processed - with a focus on cyber security.

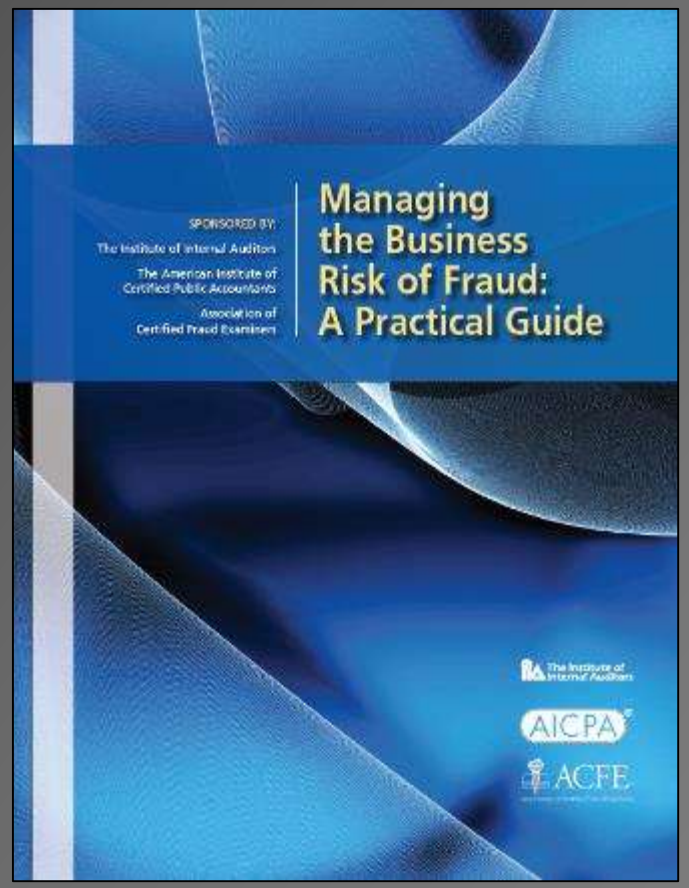
How Anti-Fraud Control May Fail

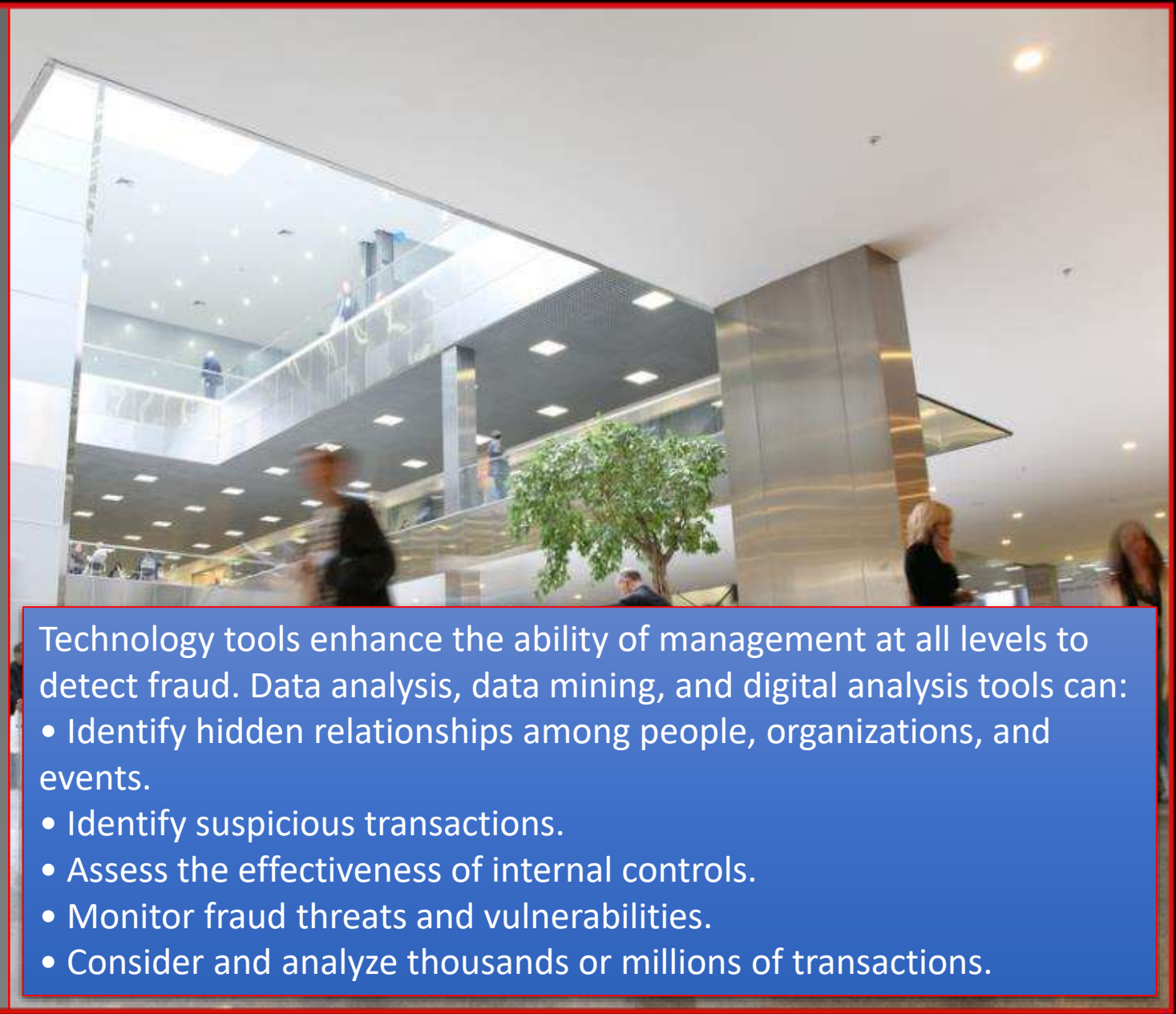
Even where we have controls in place, fraud can still arise where controls simply don't always work properly.

- Absence of astute risk culture and lack of awareness of security protocols and ID verifications where passwords are shared.
- Inadequate supervision of high risk tasks including money transfers and stock movement
- Management checks or account reconciliations not applied, and company data is not analyzed for trends & oddities
- Controls by-passed, particularly by directors and more senior people with no questions asked
- Poor segregation of duties where one person has excessive control over large transactions
- Collusion between employees or more importantly outside criminals who may even 'plant' an employee

Managing the Business Risk of Fraud

Because controls can fail, it is a good idea to regularly sweep your systems to detect irregular transactions. A quote for you.





Technology tools enhance the ability of management at all levels to detect fraud. Data analysis, data mining, and digital analysis tools can:

- Identify hidden relationships among people, organizations, and events.
- Identify suspicious transactions.
- Assess the effectiveness of internal controls.
- Monitor fraud threats and vulnerabilities.
- Consider and analyze thousands or millions of transactions.

Before we go to the next part, let me give you a concluding remark.

Fraud happens because people behave badly and controls fail. Deal with both of these issues quickly and vigorously.

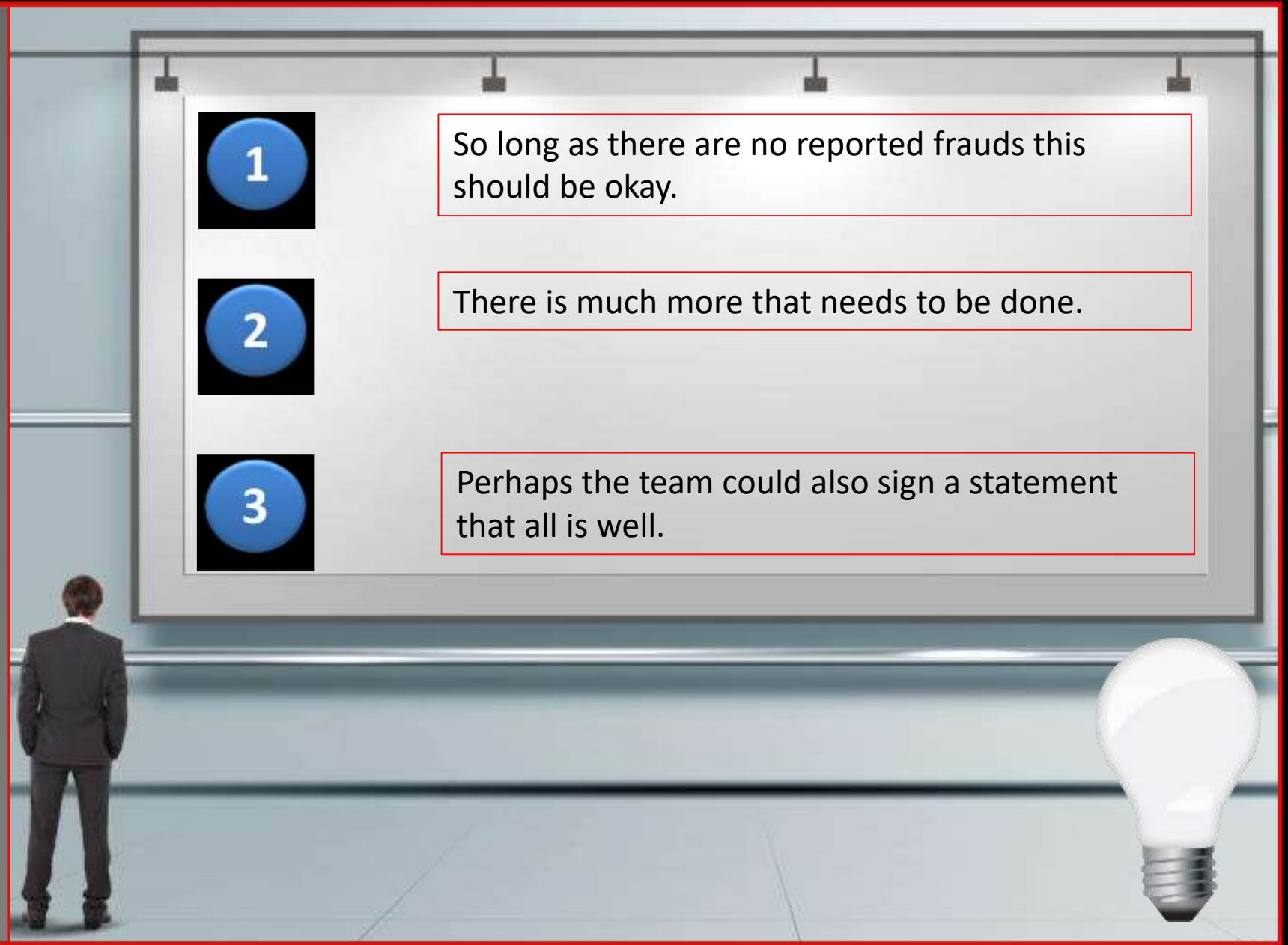
Your Tutorial

8. YOUR DYNAMIC ROLE

A Question

Your manager has just told you about a new compliance procedure where she has to provide a statement that adequate controls are in place to guard against the risk of employee fraud. She suggests you ask your team at the next meeting whether they are aware of any frauds as that should be enough to mean you can sign your fraud control statement. Would you be okay with this way of preparing your statement?

Would you chose 1, 2 or 3 as the most appropriate response? The correct answer is on the next page.



An Answer

You should tell your boss that assurances are more than just asking a few questions; they are about securing evidence that anti-fraud controls work – in that they are sound and are being observed.

We'll explore this idea in this final part of your Tutorial.

?

1 ✗ So long as there are no reported frauds this should be okay.

2 ✓ There is much more that needs to be done.

3 ✗ Perhaps the team could also sign a statement that all is well.

Weird Motives

Your fraud control plan has to be sharp enough to deal with people like a manager who was responsible for tackling on-line fraud at a large bank.

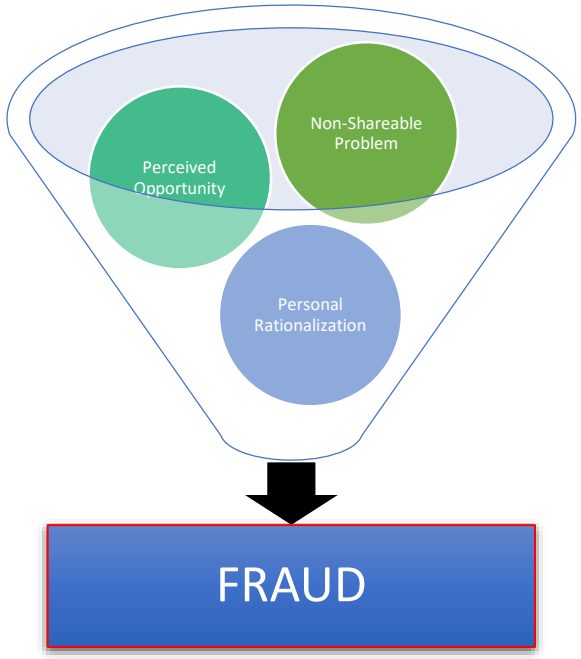
This manager stole £2.5 million by submitting forged invoices over a period of four years and was jailed for five years in September 2012.

Fraud Control Models

We will go through two models as a way of helping tackle fraud at work.

The Fraud Triangle is a well-known model that has been used for many years to aid our understanding of fraud and why it happens.

Our Stop Lights model is a simple adaptation of Red, Yellow and Green Lights to encourage employees to take a stand over wrongdoings.



The Fraud Triangle

The Stop Lights

Fraud Driver – The Fraud Triangle

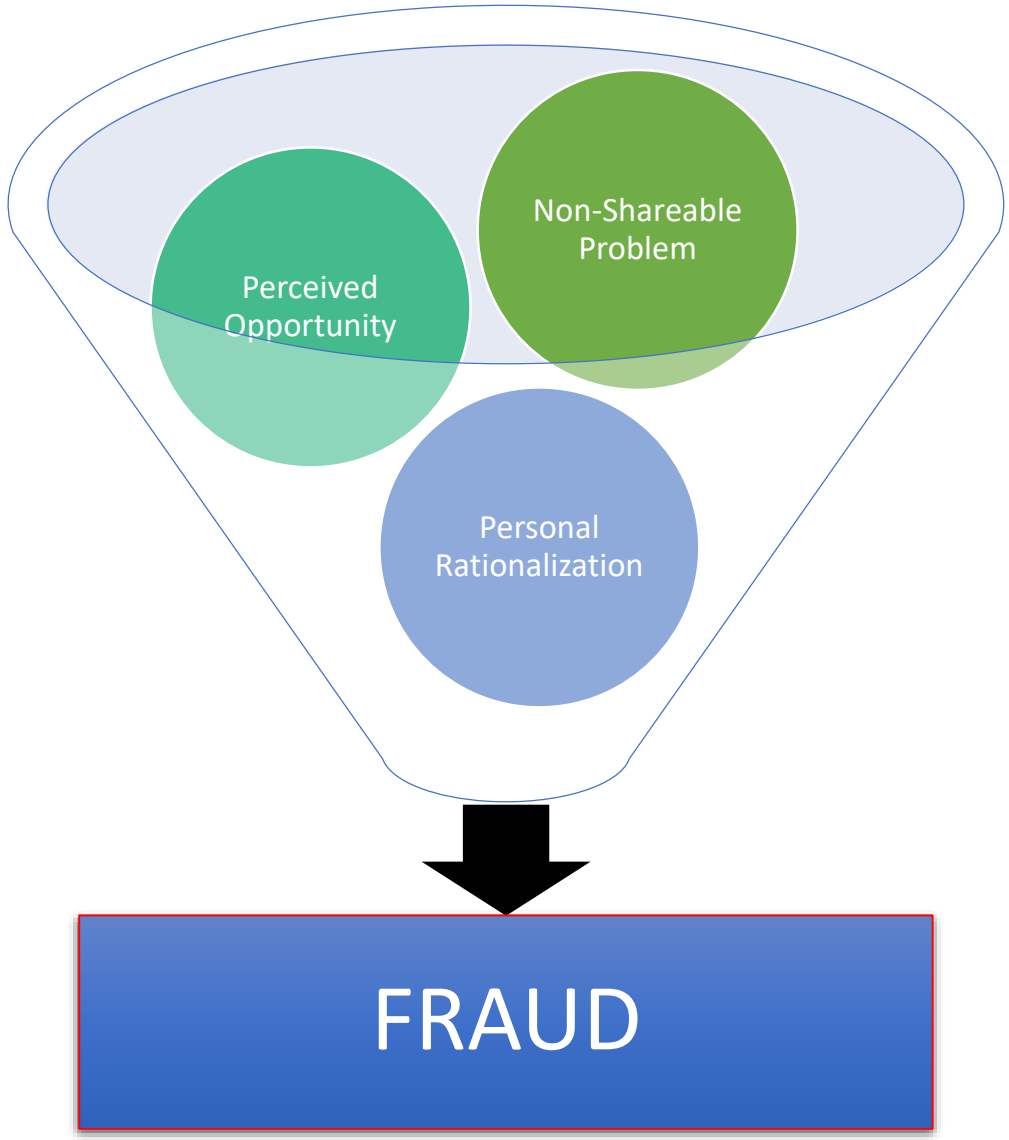
There has been a great deal of detailed research into why people commit fraud and what circumstances are required for fraud to arise, but a standard on this topic was set by Donald Cressey with three key features:

1. There must be an opportunity to commit fraud. External fraud consists of attacks on the organization from outsiders.

2. A real financial need that cannot be met from elsewhere – or shared with anyone who can help.

3. Rationalization means the person doing wrong can feel okay about it.

We have taken this excellent model and added some more detail to each of the three components over the next few pages.



The Fraud Triangle – Perceived Opportunities

Fraudsters are able to commit crime because they have an opportunity to do so. We have added three more sub-factors. Opportunity is mainly about loopholes in the system of controls that should be in place:

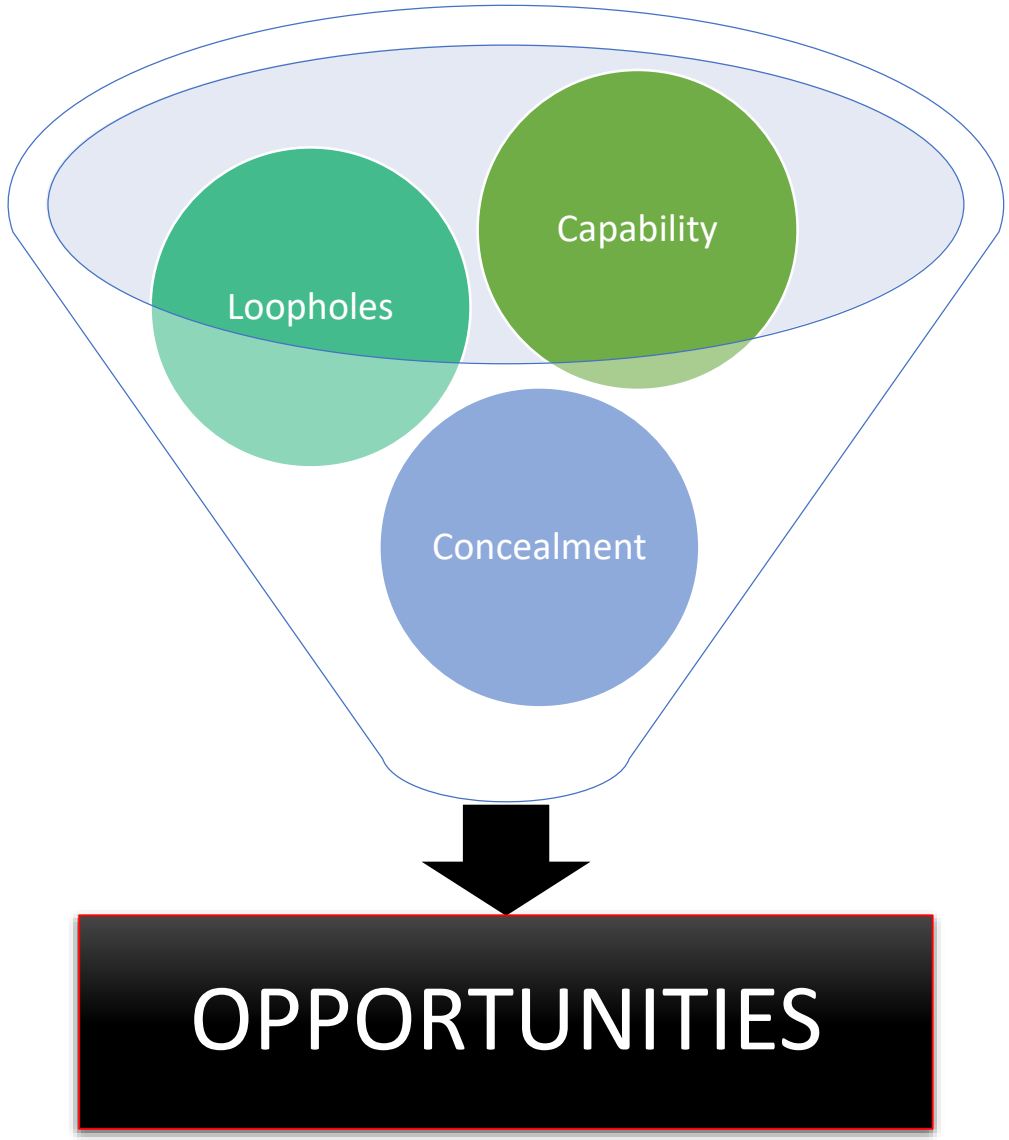
- no controls
- poor controls
- breach of control
- fatal flaws in control

The fraudster has the capability to get around the system and commit the scam:

- skilled at system
- experience of loopholes
- senior position
- trusted at work

While 'good' frauds tend to be hidden from view and concealment can go on for some time:

- falsification possible
- confused environment
- self-balancing figures
- write offs



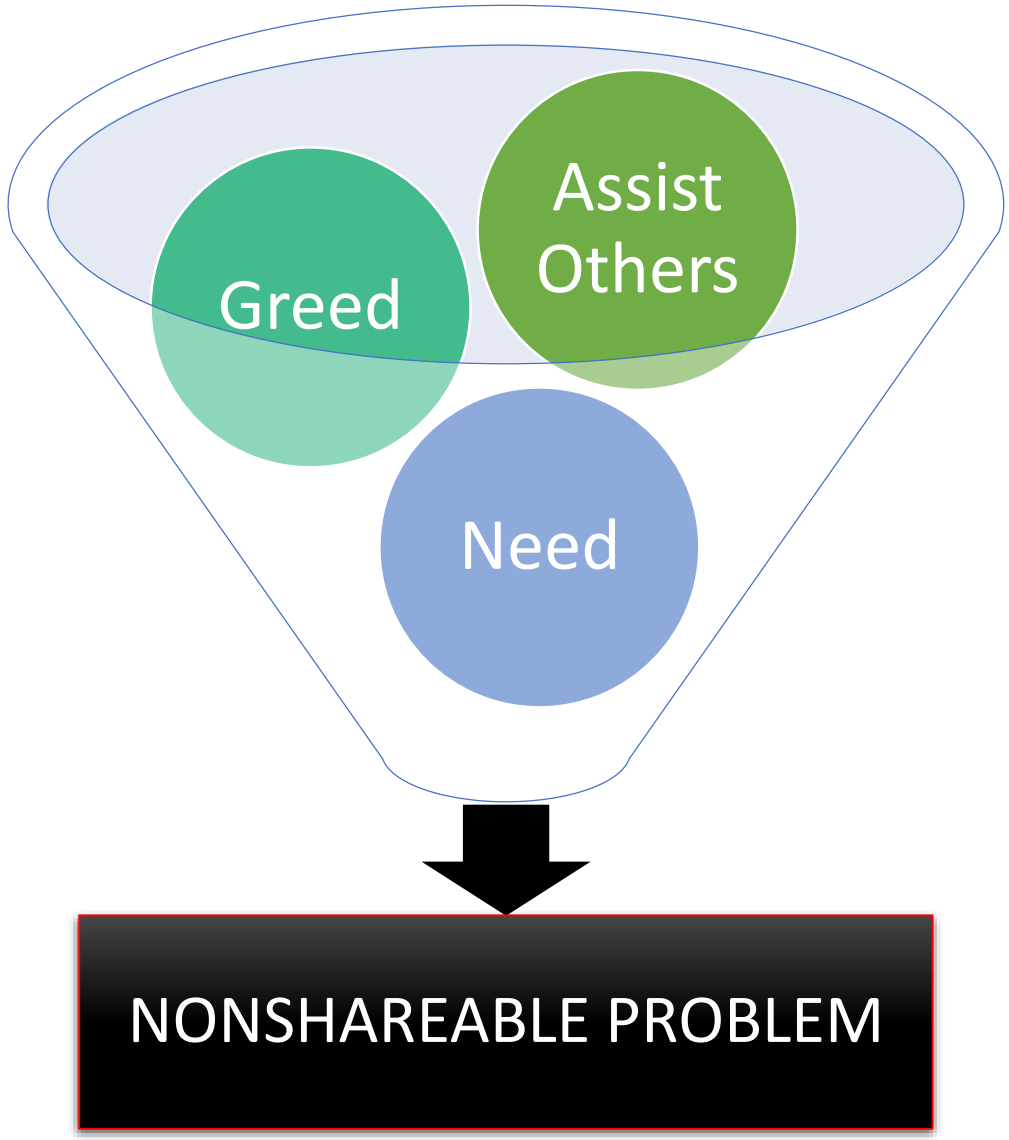
The Fraud Triangle – Non-Shareable Problem

Many people are driven to fraud because of forces they cannot share with others who may be able to offer an alternative. These forces are so strong they supersede society's view that people should be honest.

To Assist others in need of help:
- help family
- Help friends
- help colleagues
- help disadvantaged people

Sheer greed:
- status in society
- obsessive personality
- peer group pressure
- jealous of others

Or because there is a pressing need:
- gambling
- drugs
- financial crisis
- bad luck



The Fraud Triangle – Rationalization

The most scary component is rationalization, where otherwise honest people are able to convince themselves that what they are doing is excusable. We have three components:

Here fraud is seen as not an issue as everyone does it, so why not?:

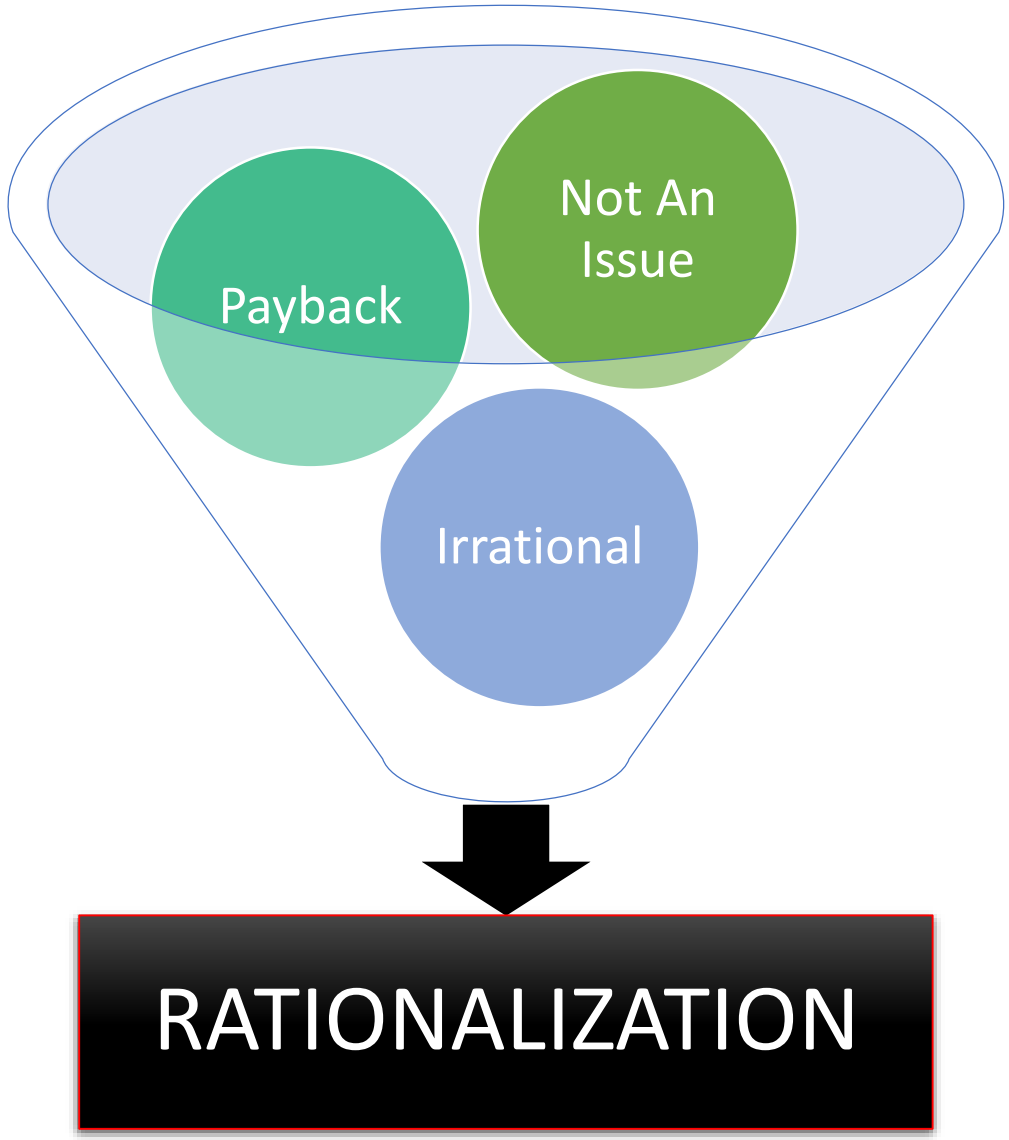
- culture of non-compliance
- managers misuse resources
- colleagues involved in scams
- seen as having no real victims

Payback means the fraudster feels they are owed whatever they take, as payback:

- overlooked for promotion
- resentment
- unclaimed expenses
- political manoeuvring

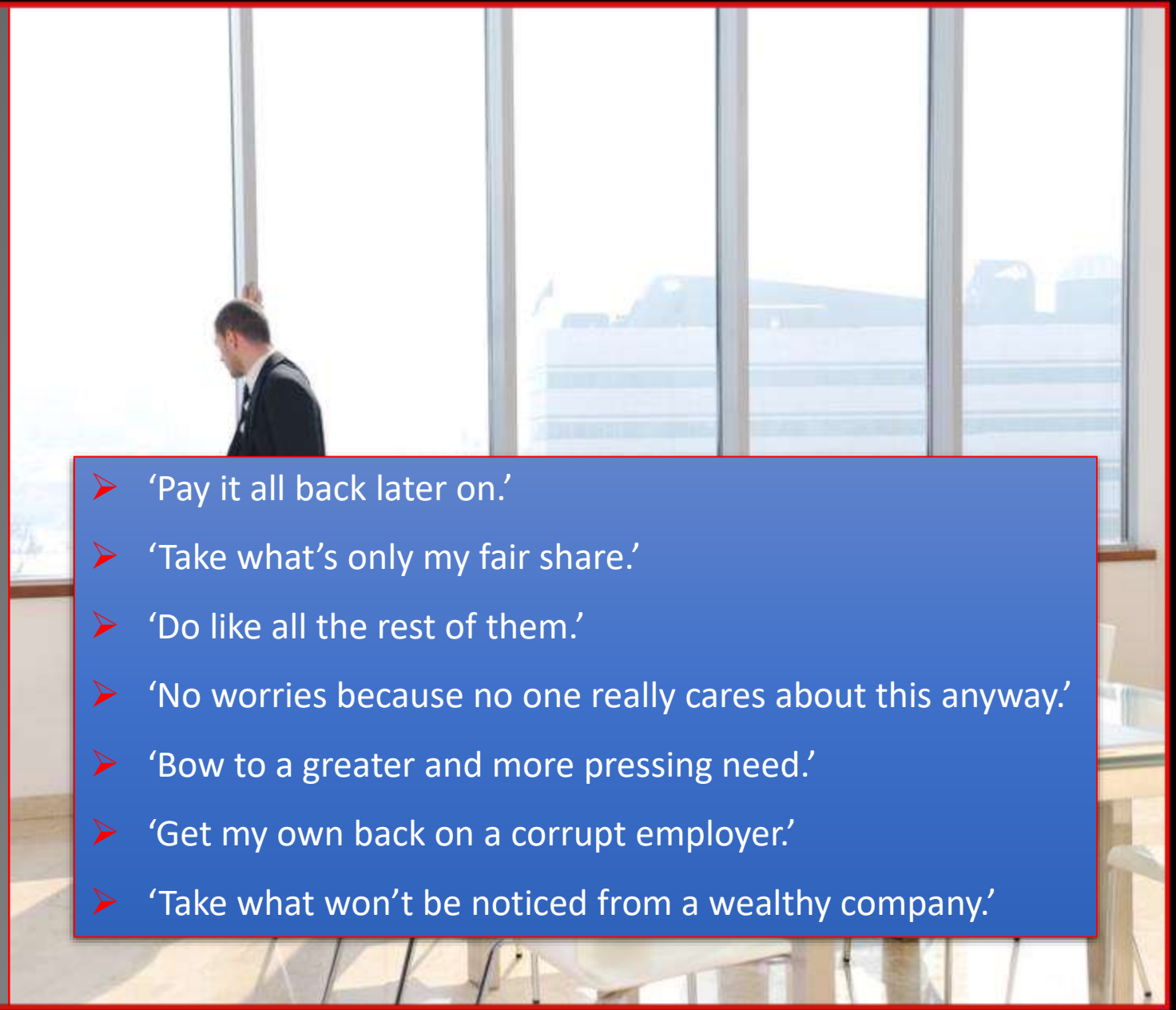
Some reasons are so irrational they make no real sense at all to reasonable people:

- no clear reasoning
- done because it can be done
- boredom at work



Rationalization

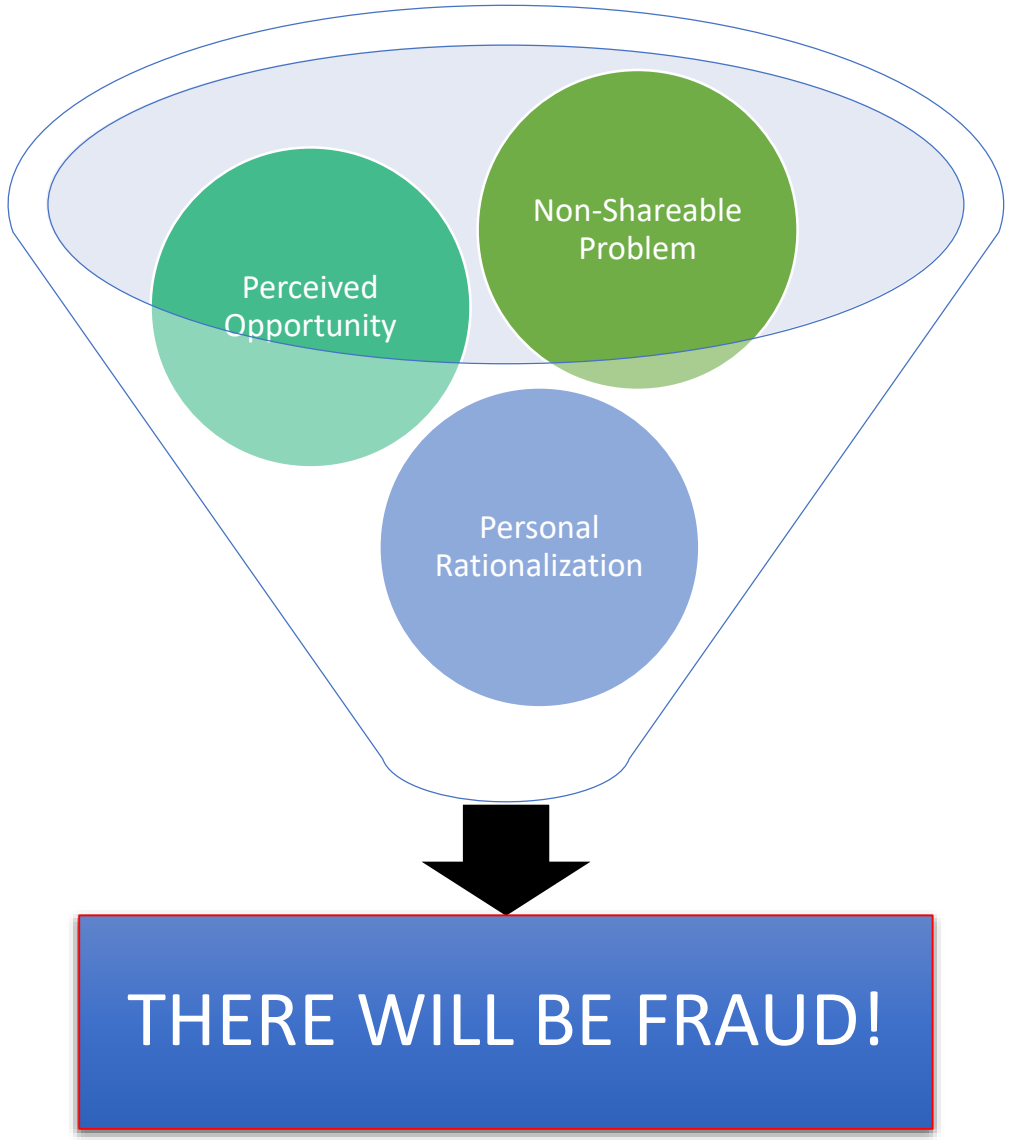
Rationalisation means an illegal action can be made to appear legitimate in someone's mind.



- 'Pay it all back later on.'
- 'Take what's only my fair share.'
- 'Do like all the rest of them.'
- 'No worries because no one really cares about this anyway.'
- 'Bow to a greater and more pressing need.'
- 'Get my own back on a corrupt employer.'
- 'Take what won't be noticed from a wealthy company.'

The Fraud Triangle – Controlling Fraud

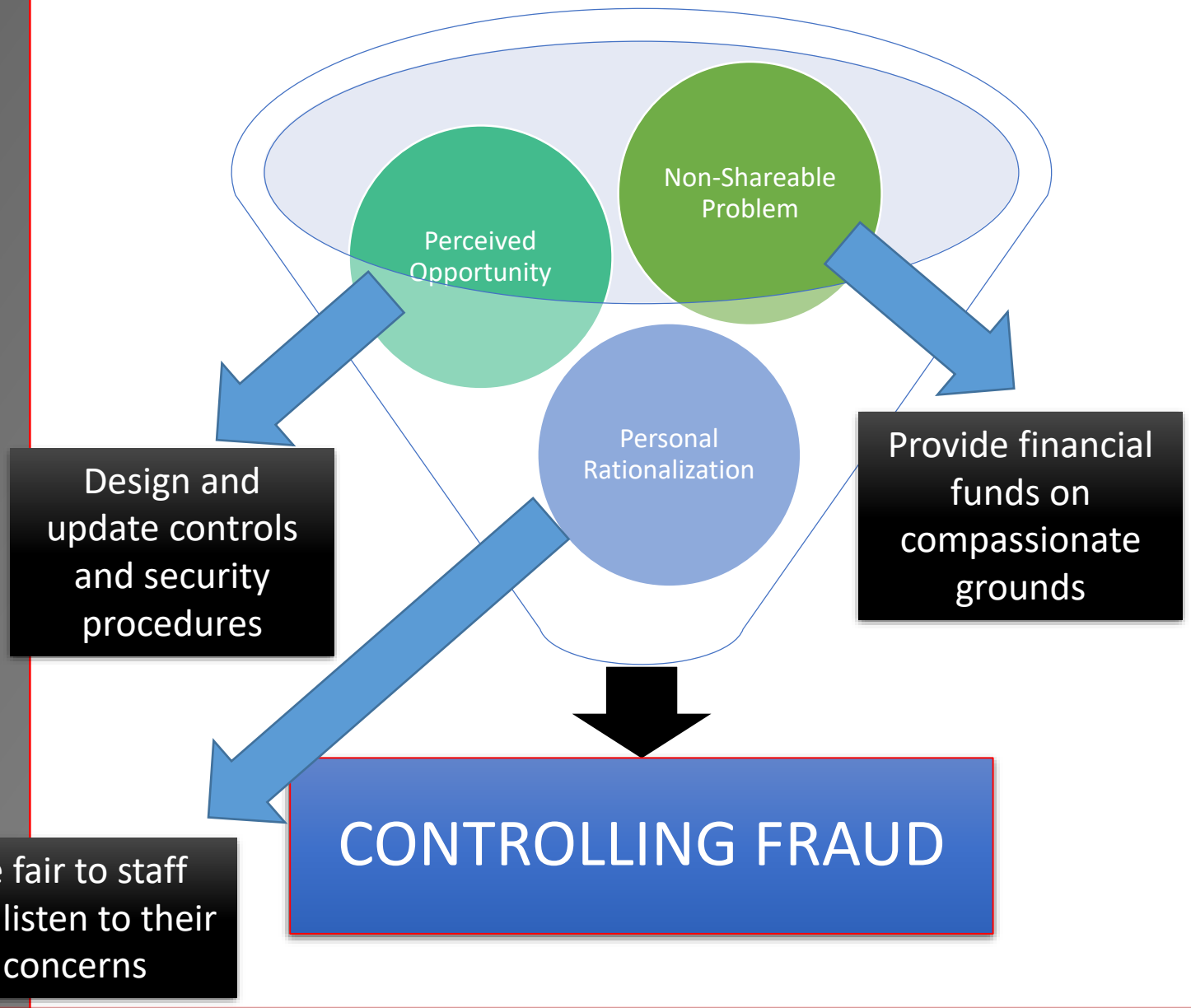
The bad news is that, if the three fraud drivers are in place there will be a strong likelihood that fraud will take place at work.



The Fraud Triangle – Controlling Fraud

The good news is that we can consider each of the three drivers and anticipate their impact. And then try to counter them as far as is possible.

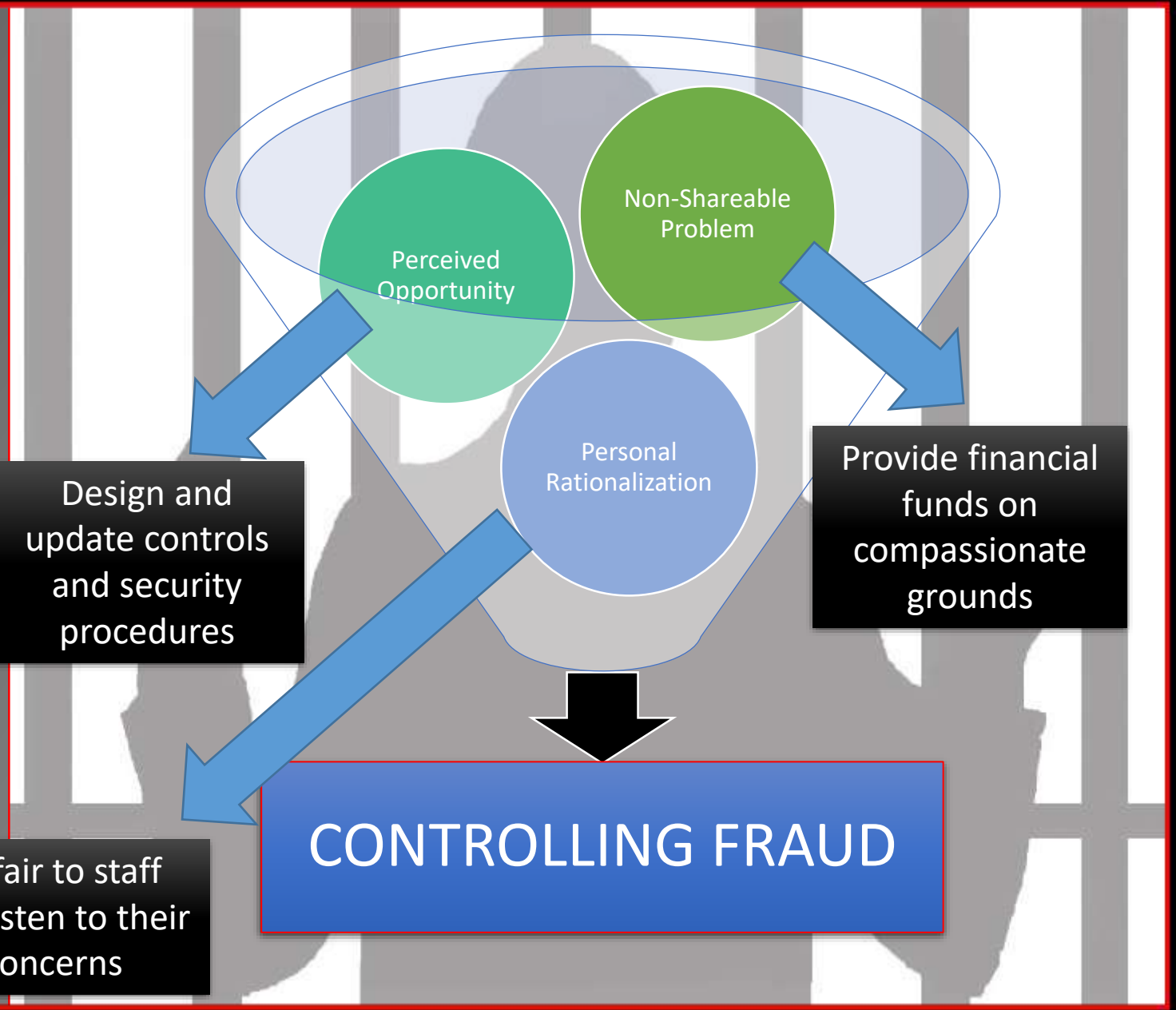
As well as using these three strands of strong controls, financial support and fair treatment.



The Fraud Triangle – Controlling Fraud

Moreover, there should be a Zero Tolerance policy in place that says fraud is unacceptable, whatever the reason.

Do not turn explanations of fraud that focus on the reasons it happens, into excuses for fraud that suggest it can ever be justified.



Your Stop Light Model

Let's go through the second model. A few want a Green Light because they are fraudsters, while many people show a Yellow light to fraud control at work as it is seen as nothing to do with them.

This has to be changed to stop fraudsters trying their luck which is about designing good controls and employing good people. We make progress by having a sound way of detecting fraud and responding to these allegations in a proactive and professional manner.

A Red Light to fraud builds on Prevent, Strengthen and Respond. It is about dealing with unacceptable CONDUCT and fixing CONTROLS so that they stop any further attacks - whenever possible. Let's recap the three colours next.

Your Stop Light Model

Let's quickly go through the three colours on your Stop Lights Model.

These are parts of the organization that are geared up to combating fraud. People at Red include specialist fraud examiners, auditors, compliance/security teams, financial controllers and others who have a clear remit to address the risk of fraud as part of their work role.

Everyone else who works for an organization is essentially at Yellow. That is, the vast majority of employees are not really concerned about the risk of fraud. They have no involvement in thinking through the potential for fraud and how this may be assessed to reduce any scope for criminality.

These are people who want a Green light to breach organizational systems. They are career criminals who have access to corporate resources including; hackers, shoplifters, credit card fraudsters and other opportunistic fraudsters who may even work for an organization they wish to defraud.

Implementing the Stop Lights

One way we can implement the Stop Lights model is to adopt a set criteria that argues that each organization should:

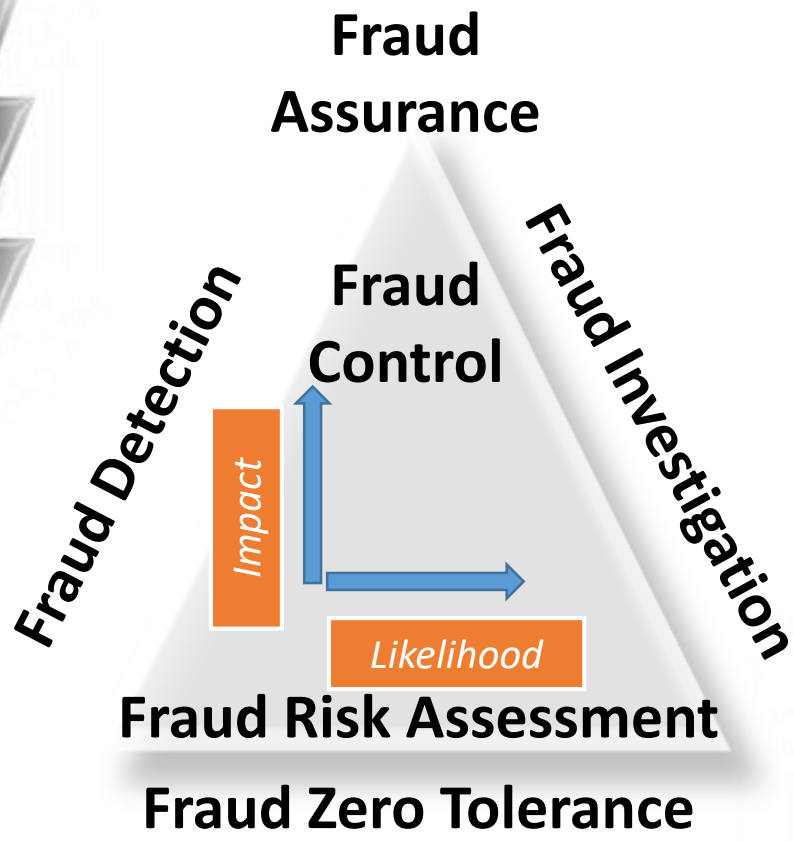
- Have a Zero Tolerance to fraud and abuse.
- Assess Fraud Risks on a regular basis
- Establish sound Fraud Controls.
- Analyse data to Detect Frauds that may be occurring.
- Investigate any actual Frauds.

What's missing from this model?

Implementing the Stop Lights

One way we can implement the Stop Lights model is to adopt a set criteria that argues that each organization should:

- Have a Zero Tolerance to fraud and abuse.
- Assess Fraud Risks on a regular basis
- Establish sound Fraud Controls.
- Analyze data to Detect Frauds that may be occurring.
- Investigate any actual Frauds.
- And then provide Assurances that you have this system in place.



Your Stop Light Model

Your stop lights model is designed to move you to a position where you incorporate the risk of fraud within the on-going risk management process for your work area - TO SHOW A BRIGHT RED LIGHT TO FRAUD.

Your Dynamic Role

Let's drill down into some of the practicalities.

The Stop Lights provide a context within which operational teams, managers and staff can assess the extent to which they are at risk from fraud and ways that they may ensure controls guard against this risk.

Your Dynamic Role

You need to assess your responsibilities at work and consider how fraud might impact your work area.

Then decide whether there is anything else they can do to help prevent, detect and generally manage the risk of fraud.

Your Dynamic Role

Next, consider the resources you may have under your control or which are affected by the way you work. We have divided these into four components. Some argue that the main threat of fraud comes from cyber crime.

Fraudsters are able to commit their crimes using remote access to corporate systems. This stage involves checking your access rights across the organization and whether these are excessive.

Your Dynamic Role

Now you need to deal with the way business fraud risks in your operations have been considered, bearing in mind what you can authorize, your approved budgets, any staff who work for you and the information systems you use at work.

Having established risk to your operations, you will then need to look at the types of control currently in place to try to prevent and detect any abuse.

Your Dynamic Role

This means you and your team need to review existing controls that focus on protecting company resources.

This is an important part of your risk assessment as it consists of asking a number of searching questions along the lines of:

'How could we be attacked by internal and, or external fraudsters and are our controls really effective in fighting fraud?'

What you do at work to control fraud should be similar to what you do for yourself.

Let's have a quick look at your own Personal Fraud Control plan.

Unfortunately unauthorized fraudsters often look, sound and appear just like authorized agents as will their web sites, phone calls, emails and correspondence.

Current Personal Risk Threats and Possible Attacks

Current Control System → **Personal Fraud Risk Review** → Personal Fraud Control

Protect Yourself

When using your personal device, there may be signs that not all is well and that you have a virus planted in your machine. Some of the more well known flags are noted here.

Every time you go online your identity is at risk as is anything you possess that can be accessed online.

The important thing is to be aware of theses risks and to protect yourself.

There is some basic guidance in the next few pages.

Pop ups suddenly appear - and may state you need to buy their software security package

Browser home page suddenly changes and takes you to strange web sites

Low disk space and very slow processing speeds

Strange messages appear at random

Computer shuts down and restarts by itself

New icons appear that you have not downloaded

Antivirus software and firewall issue alerts

Protect Yourself (Page 1 of 2)

The internet is a public network that can be accessed by anyone, in an authorized or unauthorized manner. While cloud computing means your personal data sits somewhere, on someone's computer and is also backed up. Bearing this in mind here is a quick reminder of some of the ways you can protect yourself:

1. Do not send advance fees or deposits to strangers. Advance fees may be requested for foreign lottery wins, other prizes, to buy into an investment scheme or say to release some monies that unknown to you are being held on your account (say a bequest, bank interest or royalties due to you). Request for upfront fees can arrive in the mail on impressive looking 'legal' documents. Romance scams arise when a social internet contact befriends you and eventually asks for money with a convincing explanation. Some fraudsters blackmail victims by getting them to post compromising pictures of themselves as a variation of the romance scam.
2. Keep all non-cash receipts and check your statements in detail for transactions that you did not authorize. Challenge all suspect items. Use secure payments such as PayPal or pre-paid cards and consider asking for replacements credit cards, with new card numbers periodically. Some people request a bank card with a very low credit limit for their on-line purchases to restrict any fraud risk exposure.
3. In requests for help in international disasters, only give to established charities.
4. Investment deals that promise high returns with low personal risk that look too good to be true may well be fake. 'Super deals' that have urgent deadlines with generous returns are most dangerous.
5. Watch out for companies which promise to eliminate your mortgages and other personal debt, while asking for an up-front fee for their admin services.
6. Be very careful about buying medicines over the internet. Again, only use known companies as the drugs could be fake or expired.
7. Phishing consists of attempts to obtain your personal details when you respond to emails, phone calls, or text messages. And don't click on any links that come with these messages. Keep your computer protection/anti-virus software up to date to block spam. Some companies will sell your phone number to people who may go on to contact you with a view to committing fraud. Identity theft is a growing problem where strangers get access to your personal data. This is not helped where the perpetrator uses a web site that looks like the domain used by well-known companies.

Protect Yourself (Page 2 of 2)

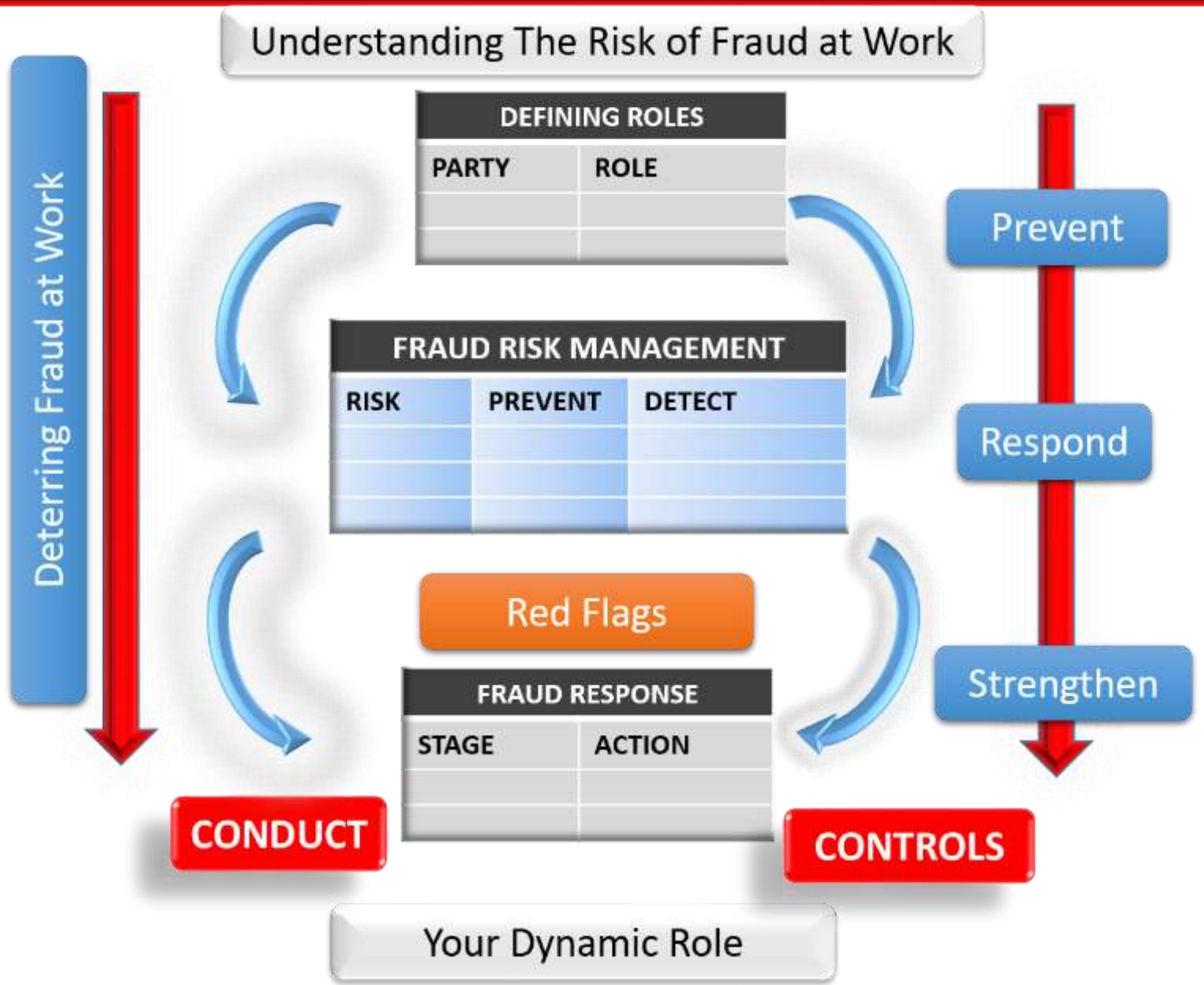
8. In general do not respond to unsolicited emails, say an attractive job offer - which should be deleted. Some job offers ask for your bank details so that your 'sign-on fee' can be sent to you. Spoofed emails appear to come from well-known companies and it is best to check with the company in question before accepting its validity. Unsolicited phone calls may be used to try to obtain your personal data, often by pretending to be from your bank's security team, tax authorities or even the police.
9. Be careful when using a public access network, say in a cafe. It may be a malicious network that redirects your data packages elsewhere. Keylogging malware records your key stokes, and then sends this information to the perpetrator.
10. Try to only use ATMs that you trust.
11. Use social media with care since it captures your personal information and some more sophisticated fraudsters spend a great deal of time compiling information on individuals that can be used for identity theft. Some people use a fake date of birth/maiden name for online systems.
12. Think about your passwords. Protect your passwords and bank/credit card details - do not record them in your diary or phone or use the same password for all your on-line systems and accounts and make sure you change them regularly. Do not use the date of birth of family members, your pet's name or your mother's maiden name. Use a mix of numeric, alpha and special characters e.g.:

    a. Find a phrase, for example:
        'The best laid plans of mice and men'
    b. Take the first letter of each word:
        t b l p o m a m
    c. Add in a few Upper cases:
        T b l p o m a M
    d. Swap a word for a special character:
        T b l p o m @ M
    e. The add few numbers (your age?):
        T b l p o m @ M 22

Also change your password regularly and do not share the details. Some systems are moving away from sole dependency on passwords to more reliable access authorizations such as voice recognition and iris, fingerprint scanning or other biometric access controls.

We've been through your Template in some detail.

Before we leave the Tutorial let's go through some closing remarks.



Your Personal Tasks

If you are happy about tackling each of the action points below, then congratulations - you are well on the way to showing a clear Red Light to fraud.

- Stick to the rules, be ethical and get approval for unusual transactions
- Ensure your anti-fraud controls work and are up to date
- Insert fraud threats in all your risk assessments
- Get advice from your internal auditors and fraud specialists
- Know your anti-fraud policy and fraud response plan
- Be aware and alert to fraud indicators, be sceptical and ask questions
- Read your Whistleblowing policy and report suspicions
- Go online and read about fraud risk management

Remember the Office Gossip?

Steve

If someone leaves and a major control is no longer operated this may create an exposure to the risk of fraud. It may be an idea to undertake a fraud risk control exercise to look at the way business loans are processed.

You could ask internal audit to undertake a fraud detection exercise to look at data that is inconsistent or indicates wrongdoing.

Since Steve left no one checks the new business loan approvals.

This could mean absolutely anything. It depends of Steve's position in the company and the context of the discussions.

Rather than jump the gun, the matter should be reported using the formal whistleblowing hot lines. Most fraudsters have no criminal record and have senior positions that mean they can access company funds.

So how come Sue said Gussy's been scamming us for ages?

Jackie

Cosy relationships with a contractor is one red flag to fraud. If Jackie makes major decisions on contacts, funding, variations and approving work, this could mean corruption is happening.

You should look out for other signs of fraud and report the matter if concerned.

Why does Jackie stop me talking to the new supplier?

Doctor

There is a form of corruption that involves drivers organizing car accidents to claim on the other party's insurance policy. The conspiracy involves securing medical opinion on 'whiplash' to support the claims.

Suspect medical practitioners will certify the injury without making any formal examination of the patient, earning fees for this fraudulent activity.

All concerns should be reported.

The new doctor is signing off loads of whiplash claims.

Orders

Money laundering is an offence and happens where money or other assets (criminal property) are exchanged for 'clean' money or other assets with no obvious link to their criminal origins.

Any concerns should be reported to the Money laundering Officer and due diligence is required to establish customers' ID and the source of funds, particularly for high risk transactions. Money laundering is sometimes linked to terrorist activity.

I wonder why Jones always pays cash for the large orders?

Payments

The Bribery Act 2010 makes the following an offence - An inducement or reward offered, promised or provided to someone to perform a relevant function or activity improperly in order to gain a personal, commercial, regulatory and/or contractual advantage, on behalf of oneself or another.

Anything that resembles a bribe should be resisted and documented then referred to the legal officer.

I'm not sure whether to pay a facilitation fee on our overseas job.

Photos

Cyber crime is now a major issue and access to information stored on computers can enable a fraudster to commit crime or pass the details onto those who would do so.

If there are strict rules on copying, printing or saving data one way of bypassing these restrictions is to use a mobile phone to photograph sensitive information.

There may be an innocent explanation but on face value, this is highly suspicious behaviour and it really needs to be followed up.

Why was Bert taking photos of his computer screen?

Zero Tolerance

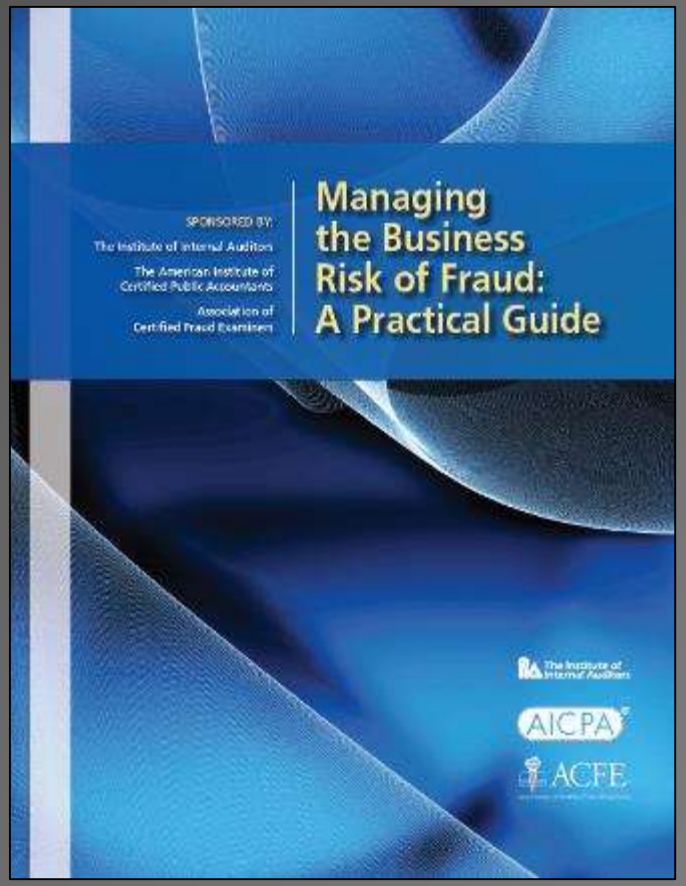
One approach to anti-fraud efforts is to use zero tolerance as the baseline, where the highest ethical standards are expected by the organization.

Many problem areas are found where lines are blurred and the rules are not always clear.

Zero tolerance is important and is about accepting nothing less.

- Having a clear and direct message on employee fraud.
- Having a position that is in the main, uncompromising.
- Setting demanding targets about what is accepted at work and what is not condoned.
- Trying to keep things one dimensional - if something appears wrong, unacceptable, or questionable; avoid it and challenge it.
- Establishing responsibility for the behaviour of staff. This responsibility lies with the individual employees and their managers.
- Matching words with action. Firm sanctions should be applied to everyone who engages in fraudulent activities.
- Asking senior people to set a good example and show leadership in encouraging the right behaviour.
- Monitoring business activities and ensuring irregularities are picked up and reported.
- Keeping staff discipline procedures vibrant and clearly linked into the corporate fraud policy.

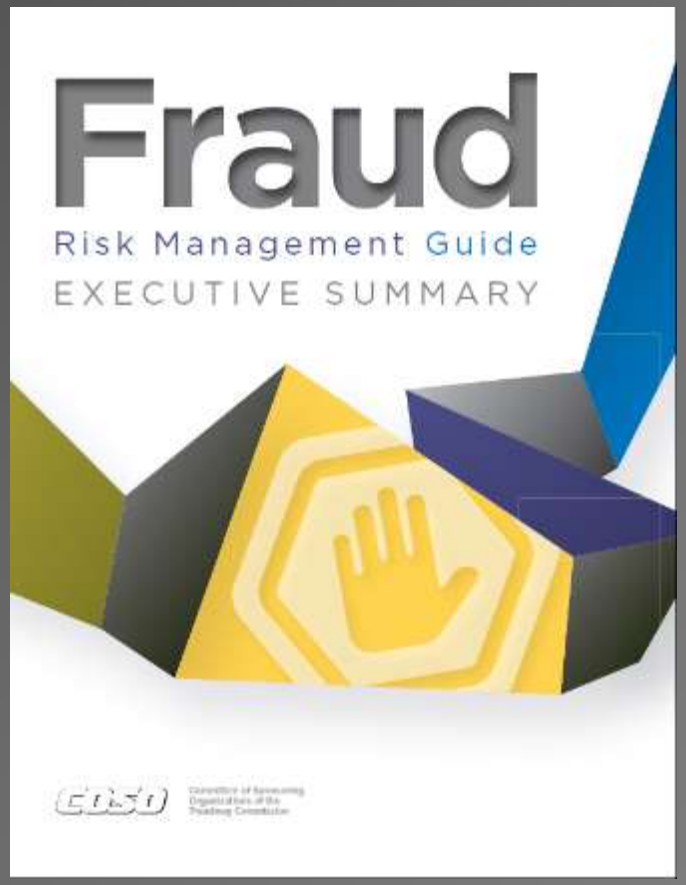
Another quote for you.



Although fraud is not a subject that any organization wants to deal with, the reality is most organizations experience fraud to some degree. The important thing to note is that dealing with fraud can be constructive, and forward-thinking, and can position an organization in a leadership role within its industry or business segment.

Managing the Business Risk of Fraud

This guide draws from and updates *Managing the Business Risk of Fraud: A Practical Guide.* The publication introduced a new model for fraud risk management in 2016.



This rigorous approach results in an ongoing, comprehensive fraud risk management process as follows:

Figure 1. Ongoing, Comprehensive Fraud Risk Management Process

What is Your Role?

You have a clear role in showing a Red Light to fraud which we have divided into four main elements.

In short:

1. Know about fraud.
2. Look out for it.
3. Deal with any suspicions.
4. Make sure it does not happen again.

Your Tutorial

SESSIONS COVERED

1. Understanding Fraud Risk
2. Defining Roles
3. Your PRS Context
4. Fraud Risk Management
5. Red Flags
6. Fraud Response
7. Conduct & Controls
8. Your Dynamic Role

Business Fraud Risk Management

Training Aims Revisited

We had one simple aim for this Training Tutorial which we hope we have achieved.

If you want to have another look at specific topics, please go to page 5 and check the List of Contents.

All The Best

I hope you enjoyed my eGuide and trust that you gained some new insights from working through the contents.

All the best from one of my favourite places; Freshwater Bay, Isle of Wight.

Goodbye.

Now you have completed your Tutorial you may wish to surf the internet for further information to build on what we have covered here.

The End