

Welcome to INF30020 Lecture 11

Internal Control & Ethics issues
- *fraud & forensic auditing*

SWINBURNE
* *
SWINBURNE
UNIVERSITY OF
TECHNOLOGY

Swinburne
▶ think forward

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

CRICOS Provider: 00111D | TOID: 3059

1

Summary, schedule and assessment

SWINBURNE Slide 2

01 August	Introduction and Overview: IS risk and security	Class activity & reading (TBA)
08 August	Information Security & risks I	Class activity & reading (TBA); Submit CLA #1, Friday 12 August
15 August	Information Security & risks II	Class activity & reading (TBA)
22 August	Identifying Information Assets & evaluating risks	Class activity & reading (TBA); Submit CLA #2, Friday 26 August
29 August	Mitigation, treatment & control I	Class activity & reading (TBA)
05 September	Mitigation, treatment & control II	Class activity & reading (TBA); Submit Online Quiz #1, Friday 08 September
19 September	Information Security & Information Governance	Group Warm-up (TBA); Submit in class, Wednesday 21 September
26 September	Business Continuity Management	Class activity & reading (TBA);
03 October	Contingency Planning	Class activity & reading (TBA); Submit CLA #3, Friday 07 October
10 October	Cybersecurity and Business Continuity Management	Class activity & reading (TBA);
17 October	Fraud and forensic auditing: Fraud, cybercrime, forensic auditing and continuous monitoring	Class activity & reading (TBA); Submit Report Part B, Friday 21 October
24 October	Information Security ethics, compliance and pre-quiz revision	Class activity & reading (TBA); Submit Online Quiz #2, Friday 28 October

Classes

- 1 x 2hr F2F Workshops across the semester, Weds 8:30, 10:30
- M001 – M009 completed

Assessments

- CLA#1 , CLA#2 submitted and returned marking, **CLA#3 marking underway**
- Group warm up exercise completed (those present receive mark)
- Quiz 1 completed, **Quiz 2 next week!**

Groups

- **Group assignment**
 - was due Friday 21 October, 11:59pm
 - **Now due Tuesday 25 October, 9am**

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

2

Whitman Chapter 12

SWIN
BUR
NE

Slide 3

Internal controls for risk mitigation strategies

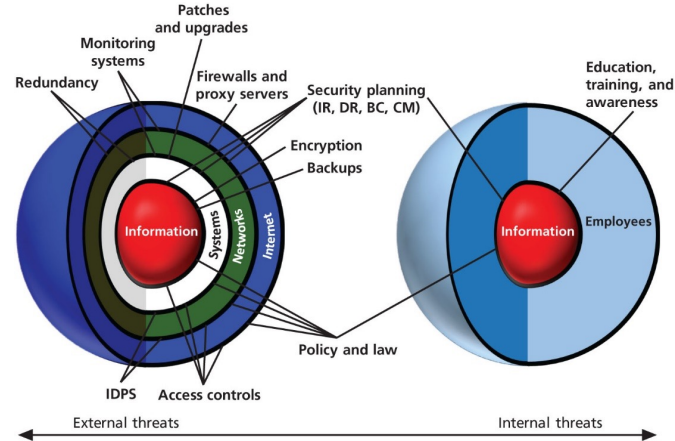


Figure 12-1 Sphere of security

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

3

Internal controls for risk mitigation strategies

SWIN
BUR
NE

Slide 4

Access controls	regulate the admission of users into trusted areas of the organization, logical & physical encompassing, Identification , Authentication Authorisation, Accountability including Network access control
Firewall	any device that prevents flagged information from moving between the outside world, untrusted network (e.g., the Internet), and the inside world, known as the trusted network
Intrusion Detection & Prevention Systems (IDPS)	work like burglar alarms, range of detection & monitoring methods that react to changes in the environment, which is available in intrusion prevention technology (stopping connection, blocking access, isolating, quarantine)
Scanning & analysis tools	find vulnerabilities in systems, holes in security components, and other unsecured aspects of the network (port scanning for active computers on a network, packet sniffing)
Log monitoring	A security event information management, i.e. records of activity in systems
Encryption	converting an original message into a form that cannot be understood by unauthorized individuals (email security, web security e.g. SSL, IP security)

Whitman Chapter 12

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

4

Moving forward



Today's topics: Fraud and forensic auditing



"IF THEY ONLY
USED THEIR
GENIUS FOR GOOD
INSTEAD OF EVIL"
Batman

Batman is cited in 'Foiling Internet Fraudsters', *Fraud Magazine*, March/ April 2005.
Image from Google Image database, May 2015

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

5

Reading for this week's learning plan

- (1) This week's topic area is not a strength of our unit texts.
- (2) It is our expectation that most students are concentrating on the group assignment and the associated readings and learning plan from week's 5-10 , and especially 7-10
- (3) When preparing for Challenge Quiz 2 , your best source for *Fraud & forensic auditing* will be this lecture & the accompanying slides

Unit texts:

- Whitman, Michael E. and Mattord, Herbert J. Chapter 2, Compliance, Law and Ethics. *Management of information security*. Sixth Edition., Stamford, Conn. : Cengage Learning, 2018.
- Gibson, Daril, Chapter 3. Maintaining Compliance, *Managing Risk in Information Systems*. 2015.

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

6

This weeks' learning plan



Gain an understanding of

1. What constitutes fraud (especially in terms of cybercrime)
2. The significance of organisational fraud in Information Systems security management
3. Approaches to identifying and controlling against fraud
4. *Computer assisted auditing techniques and tools (CAATTs), extension slides available*

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

7

Fraud & cybercrime



Cybercrime

Cybercrime takes two forms:

1. crimes *where computers* or other information communications technologies *are an integral part of an offence* (such as online fraud, identity theft, the distribution of child exploitation material)

The term 'online fraud' refers to any type of fraud scheme that uses email, web sites, chat rooms or message boards to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme.

2. crimes *directed at computers* or other information communications technologies (such as hacking or unauthorised access to data – “self-proclaimed leader of an international hacking ring Matthew Flannery”).

Australian Criminal Intelligence Commission

<https://www.acic.gov.au/about-crime/organised-crime-groups/cybercrime>

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

8

Use of computers to commit a crime

- Internet banking fraud
- Phishing attacks
- Shopping and auction site fraud
- Online mule recruitment
- Scams, Nigerian lottery, inheritance
- 2000 coronavirus-specific scam reports with over \$700 000 in reported losses from the scams

Online enrolment applications.

June 2018, former Auburn (NSW) deputy mayor Salim Mehajer, convicted of more than 100 charges relating to forging documents or giving false or misleading information to the Australian Electoral Commission

"...the applications came from computer IP addresses associated with the Mehajer family and that the siblings had exchanged numerous text messages about the fraud in the lead up to July 31."



SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

9

Fraud & organisational fraud

A fraud is

The misrepresentation of a material fact made by one party to another party **with the intent to deceive and induce the other party to justifiably rely on the fact to his or her detriment**. It must meet the following five conditions:

1. False representation – a false statement or non-disclosure
2. Material fact – a substantial factor in inducing someone to act
3. Intent – there must be the intent to deceive or knowledge that the statement is false
4. Justifiable reliance – the misrepresentation must be a substantial factor on which the injured party relied
5. The deception or loss must have caused injury to the victim of the fraud

e.g. Andy Fastow, Enron

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

10

Organisational fraud

SWINBURNE
Slide 11

The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organisations resources and assets

Association of Certified Fraud Examiners (USA), Report to the Nation on Occupational Fraud & Abuse, 2014

- An intentional deception, misappropriation of company assets, or manipulation of its financial data to the advantage of the perpetrator
- **White collar crime**, usually comprising two levels:
 - Management fraud
 - Employee fraud

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

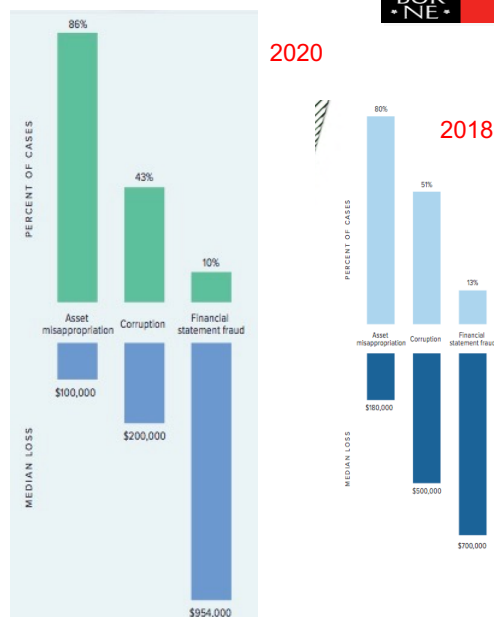
SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

11

Organisational fraud

How organisational (aka occupational) fraud is committed?

Charts from: Association of Certified Fraud Examiners (2018 & 2020), ACFE Report to the Nation on Occupational Fraud & Abuse 2018-2020



SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

12

Organisational fraud



White collar crime, as comprising two levels:

1. Employee fraud usually involves:

Stealing something of value; converting an asset to a usable form; concealing the crime to avoid detection

2. Management Fraud:

Often takes on some form of *manipulation of performance value* e.g. to obtain higher stock values – to improve position of stock in their management portfolio; inflate advantages or assets to meet stockholder and reporting requirements;

Usually occurs at levels above that at which internal controls have impacts; materially mistating financial data; can involve complex business transactions involving third parties

What motivates the fraud – situational pressures; opportunities; personal characteristics (e.g. integrity)

Enron – when systematic fraud takes place: “recorded assets and profits were inflated or even wholly fraudulent and nonexistent.” Entities established to hide loss. Auditors involved in inaccurate and destruction of records

<https://www.youtube.com/watch?v=Mt2O1bH8pvw>

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

13

Organisational fraud



“imagine what the world would be like if elevators were not built so that people could inspect them..”

“Proprietary software is an unsafe building material,” Mr. Moglen had said. “You can’t inspect it.”

Columbia University Law Professor Ebin Moglen, speaking on issues associated with the dangers of *Secret Code*, 2010: *illegal defeat devices*

Is software an active space for fraud: Volkswagen emissions scandal 2015, 11 million cars worldwide: The software sensed when the car was being tested and then activated equipment that reduced emissions,but the software turned the equipment off during regular driving, increasing emissions far above legal limits, possibly to save fuel or to improve the car's torque and acceleration.

Prosecutors would have to prove that the Volkswagen employees distorted facts to trick people into buying their cars. Volkswagen has been promoting itself as a sustainable automaker for years, and its “clean diesel” cars were a hit with customers.

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

14

VW lawyers sought to exonerate management

VW, a former paragon of German industry with ambitions to become the world's biggest carmaker, has been plunged into its deepest-ever crisis by [revelations that it installed emissions-cheating software into 11 million diesel engines worldwide](#).

On top of still unquantifiable regulatory fines in a range of countries, VW is facing a slew of legal suits from angry car owners, as well as from shareholders seeking damages for the massive loss in the value of their shares since September.

VW has insisted from the very beginning that a [small group of engineers was behind the scam](#).


And in a copy of the defence document obtained by AFP, VW's lawyers sought to exonerate the group's management in the affair, including former chief executive Martin Winterkorn and other board members, such as current supervisory board chief Hans Dieter Poetsch.

It conceded that discussions had been held and memos exchanged at top management level, but the issue was simply one of a number of others for board members.

Mr Winterkorn, who resigned in the wake of the affair, may have been warned as early as May 2014 of possible anomalies dogging its diesel engines, 16 months before the scandal erupted worldwide, the company admitted.

However, none of its top bosses could have known of the full extent of the scandal until it broke in September 2015, VW argued.

How VW's 'defeat device' worked



[How did German carmaker Volkswagen rig emissions tests in diesel-powered vehicles and fool US regulators?](#)

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

15

Is software an active space for fraud?

Banks and law enforcement agencies are applying KDD, data mining and AI effectively for credit card fraud detection

Outlier analysis: opposite to commonality models (above), proposes that outlier point to meaningful abnormalities e.g. abnormal transactions as an indicator of fraud

Banks are finding that **AI for fraud detection is fast, effective and efficient**. In 2021, Fintech News reported that financial institutions are deploying AI-based systems in record numbers, with more than \$217 billion spent on AI applications to help prevent fraud and assess risk.

AI is also an active space for fraud: applying AI to brute force attacks that

- (1) automatically generate and try username/password combinations.
- (2) discover matches between personal information and credit card details correct enough to evade fraud detection and add to the "good quality" sales list. When the list of The speed of the algorithm makes it much easier to find large numbers of matches very quickly.

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

16

Organisational fraud

SWINBURNE
Slide 17

Organisational fraud is often hard to detect (the median length of a fraud scheme in the ACFE study for 2020 was 16 months)



Frauds that last over 60 months are 20 times more costly than those caught in the first 6 months

Fraudsters usually start small and increase rapidly in the first three years

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

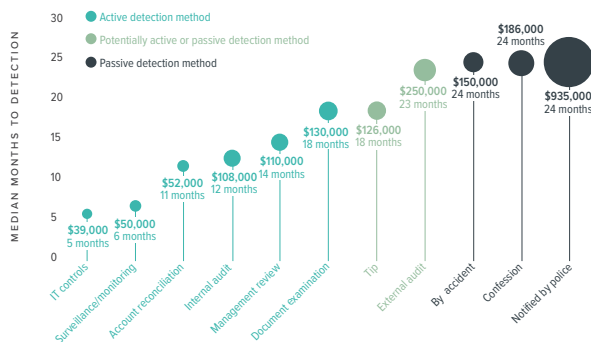
17

Organisational fraud

SWINBURNE
Slide 18

One of the most visible distinctions is that the five detection methods with both the shortest duration and lowest loss for a fraud event — IT Controls, surveillance/monitoring, account reconciliation, internal audit and management review — involved proactive efforts to discover fraud

FIG. 11 How does detection method relate to fraud duration and loss?



Checklists for Key Executive: the red flags

- Unusually high personal debt?
- Living beyond means?
- Habitual gambling?
- Alcohol or drug abuse?
- Economic climate for industry?
- Company using multiple banks
- Close association with suppliers
- Rapid turnover of other senior staff
- 1 or 2 individuals dominating the company

Charts from: Association of Certified Fraud Examiners (2020), ACFE Report to the Nation on Occupational Fraud & Abuse 2020

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

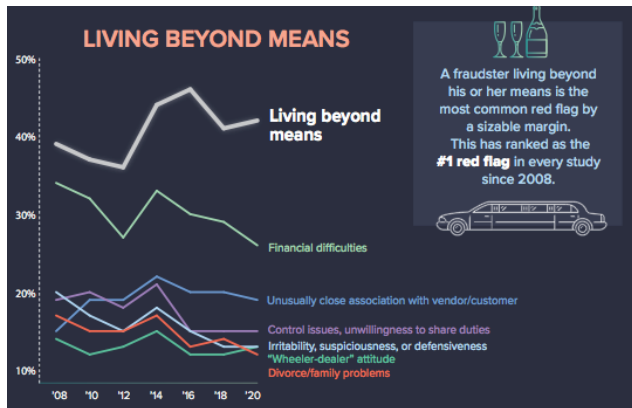
SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

18

Organisational fraud

SWINBURNE
Slide 19

85% OF ALL FRAUDSTERS displayed at least one **BEHAVIORAL RED FLAG** while committing their crimes.



Charts from: Association of Certified Fraud Examiners (2020), ACFE Report to the Nation on Occupational Fraud & Abuse 2020

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

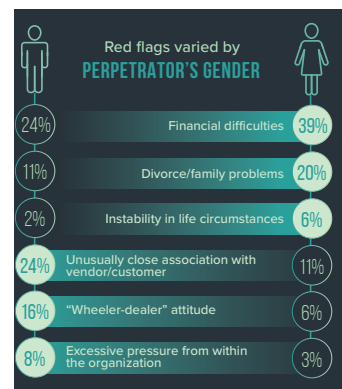
The "Bank of Carolyn" 2001 – 2013. Carolyn Hanigan, a secretary for a Melbourne based suburban signwriting company, whose duties included invoicing, filing, paying bills and wages and reconciling accounts, stole \$363,722 on 198 separate occasions by concealing the thefts in false invoices. *16 plus month jail sentence*

19

Organisational fraud

SWINBURNE
Slide 20

- Small business suffer disproportionately high losses (MEDIAN \$200k versus 104K): commonly through employees writing company cheques, skimming revenue, processing fraudulent invoices
- Small business **not proactive** against fraud – large number with fraud detecting processes, internal audit departments, without established controls, little or no training and awareness
- **Predominately males (Greater than 73% in Asia Pacific , including Australia)**
- **Direct correlation between tenure and fraud. Employees with firms longer than 10 yrs likely to be more senior and more likely to commit larger (\$) frauds**



Charts from: Association of Certified Fraud Examiners (2020), ACFE Report to the Nation on Occupational Fraud & Abuse 2020

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

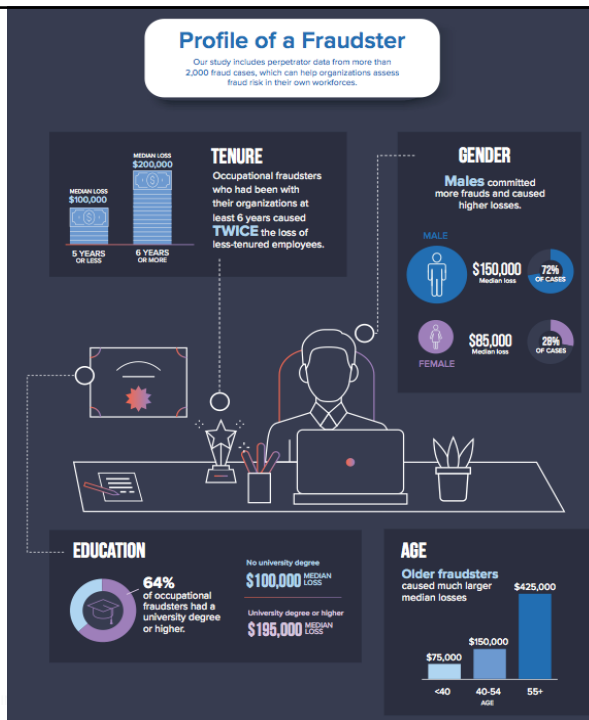
20

Organisational fraud

- **Direct correlation between tenure and fraud. Employees with firms longer than 10 yrs likely to be more senior and more likely to commit larger (\$) frauds**

And there are exceptions to the rule *Elizabeth Holmes & Theranos*:
<https://www.youtube.com/watch?v=Y0e778c2Bg0>

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS



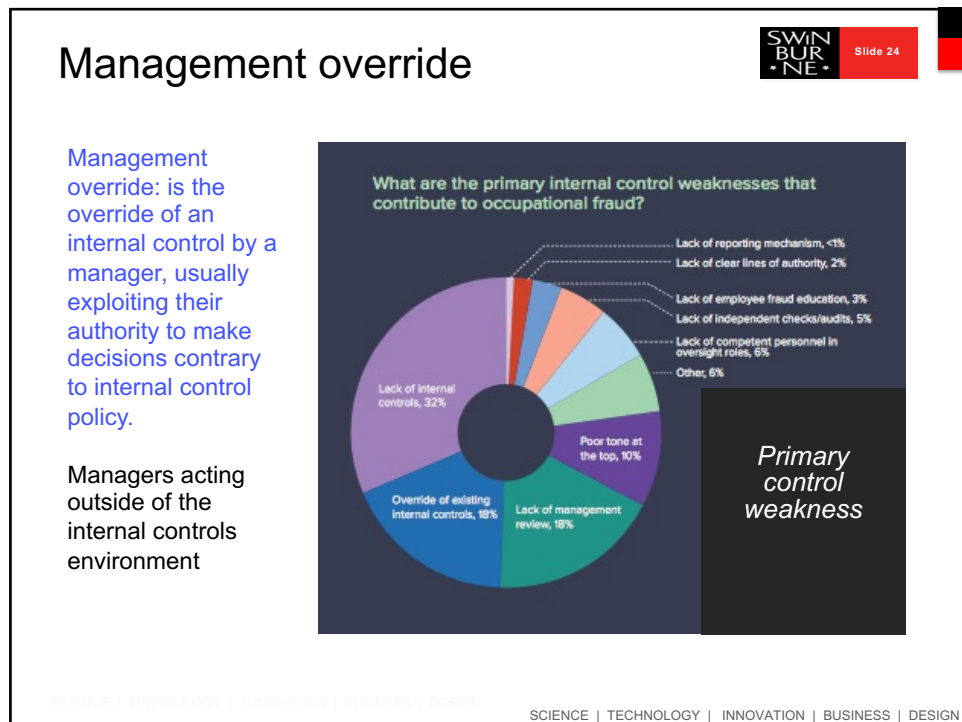
21



22



23



24

Organisational fraud



Who is responsible for prevention, detection, and reporting?

- **Management is responsible** for the prevention and detection of any irregular and illegal acts in an organisation, *not IS security or the IS auditor.*
- However ASA 240 (Auditing and Assurance Standards Board) - The Auditor's Responsibility to Consider Fraud in an Audit of a Financial Report
 - *Maintain an attitude of professional skepticism*
 - *Perform procedures to obtain information that is used to identify and assess the risks of material misstatement due to fraud*
- And it is clear that it must be considered a responsibility of Internal Audit departments
 - Lack of auditor independence
 - Lack of director independence

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

25

Organisational fraud



Overview of IS audit responsibilities

- Plan the IS audit engagement based on an assessed level of risk that **irregular** and **illegal** acts might occur
- *Professional skepticism means, designing and implementing IT audit procedures that consider the assessed risk level for both irregular and illegal acts.*
- Review the results of audit procedures for indications of irregular and illegal acts.
- Report suspected irregular and illegal acts to one or more of the following parties – immediate supervisor (or one step above) or to an external authority

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

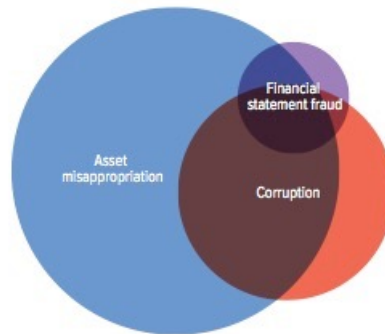
26

Organisational fraud

SWINBURNE
Slide 27

Fraud schemes

1. Fraudulent (mis)statement
 - Falsification of an organisations financial statements. Must bring some material benefit to the perpetrator
2. Asset Misappropriation
3. Corruption



SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

27

Organisational fraud

SWINBURNE
Slide 28

Corruption

- Wrongful or unlawful use of position to procure a benefit for yourself or another
 - ACFE asserts corruption accounts for over 10% of fraud cases
 - Bribery – offering or receiving things of value to influence an official in the performance of their duties
 - Illegal gratuity – offering or receiving something of value for an act that was undertaken. Similar to a bribe but the transaction occurs after the act
 - Conflicts of interests – acting on behalf of a third party during the discharge of your duties. Both bribery and gratuities constitute a conflict of interest, however a conflict of interest can be present without these two reward processes in place

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

28

Organisational fraud



Corruption

Siemens AG

Siemens, German parent company / engineering firm, ran afoul of the law in 2008 when it was charged for paying \$16 million to the president of Argentina to secure a contract for making Argentinean **digital identity cards**. The contract was worth \$1 billion to Siemens AG. In total, the company was accused of paying more than \$100 million in total to government officials.⁷ Eight former employees and contractors were charged in the scheme.⁸ Siemens settled with the Department of Justice and paid \$1.6 billion in fines in the U.S. and Germany

Former Siemens AG employee pleaded guilty on Thursday to a U.S. charge that he took part in a bribery scheme to win a contract for the German engineering company to make national identity cards for Argentina's government.

Eberhard Reichert, a 78-year-old German citizen, employed at Siemens since 1964, Reuters

Between 2010 – 2022, other companies caught in ID contract bribery include Semlex, GmbH, Laynes

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

29

Organisational fraud



Corruption

- Wrongful or unlawful use of position to procure a benefit for yourself or another

Apple employees in Ireland offered €20,000 in bribes to pass login IDs to hackers



By Mary-Ann Russon
February 10, 2016 13:30 GMT



"you'd be surprised how many people get on to us, just random Apple employees," the source said. "You get emails offering you thousands to get a password to get access to Apple. I could sell my Apple ID login information online for €20,000 (£15,000 / \$23,000) tomorrow. That's how much people are trying."

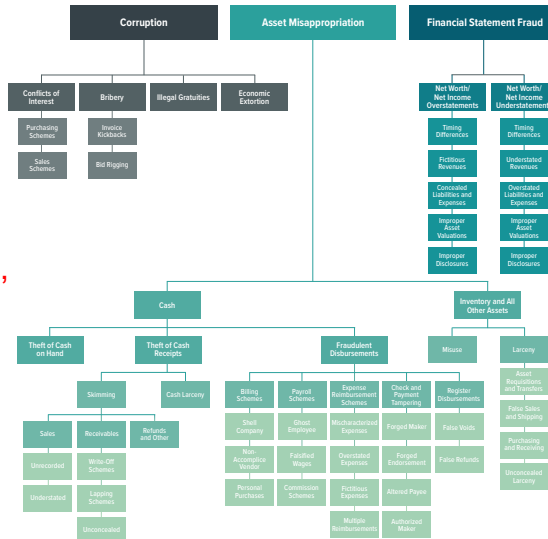
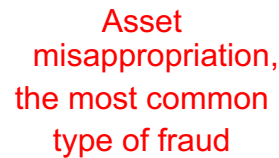
SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

30

Organisational fraud

SWINBURNE
Slide 31



SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

31

Organisational fraud

SWINBURNE
Slide 32

Asset misappropriation

- The most common way to hide an imbalance between assets and equities is to hide a theft by transferring it to another account, e.g. an expense account (**Jerome Kerviel, 4.9 billion Euro in losses**)
<https://www.independent.co.uk/news/world/europe/french-rogue-trader-jerome-kerviel-found-guilty-of-fraud-2098068.html>
<https://www.youtube.com/watch?v=gPCfX2KYsfs>
- **Lapping**, using money from a customers account and then using ongoing deposits of customers to hide the loss (in a rob Peter-to pay Paul model; often rationalised by perpetrator an intent to repay)
- **Skimming**, in which cash is taken before it is recorded on the books (accept payment but do not record the sale)
- Cash larceny, stealing cash after it is recorded but before it is deposited
- **Transaction fraud**, deleting, altering or adding false transactions e.g. the distribution of fraudulent cheques (paying non-existent employees)
- Others, cheque tampering, wire transfer, expense reimbursement, other payroll schemes

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

32

Organisational fraud



Computer fraud schemes

- The theft, misuse or misappropriation of assets
 - by altering computer readable records or files
 - by altering the logic of computer software
- The theft or misuse of computer readable information, or software and hardware
- The simplest way to perpetrate a computer assisted fraud is at the data collection stage. e.g. falsifying data at the data entry stage. It is the computer equivalent of a transaction fraud – adding, altering, deleting transaction information
- Masquerading: access from a remote site by pretending to be an authorised user
- Piggybacking: latching on to a remote user as they log-in to a system (constant monitoring for an opening) ,, intentional access of an open Wi-Fi network with harmful intent

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

33

Organisational fraud



Computer fraud schemes

- Piggybacking: latching on to a remote user as they log-in to a system (constant monitoring for an opening) ,, intentional access of an open Wi-Fi network with harmful intent
- In Singapore in May 20007,
- Lin Zhenghuang was sentenced to three months' imprisonment and fined 4,000 US dollars (2,614 US). He had posted an online bomb hoax while piggybacking on a neighbour's wireless network.
- Fireball browser hijacking malware piggybacked on legitimate software downloads from Beijing digital marketing company named Rafotech, Rafotech employees/hackers had earned more than 80 million yuan (\$11.84 million) generating fake clicks and traffic to other websites, reportedly up to 250 million computers

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

34

Organisational fraud

SWINBURNE
Slide 35

Data processing

- Program fraud
 - creating illegal programs / altering program logic, that can access data files to alter, delete or insert values to records, process data incorrectly
 - destroying or corrupting program logic by virus
 - rounding frauds associated with complex routines for interests calculations. In Banking systems fractional amounts are usually held over in a 'memory accumulator' Whole cents are added and subtracted randomly against customer accounts but the total interest charges and credits are kept in balance. Rounding frauds modify the algorithm to always add the positive rounding to the customers account
- Operations fraud
 - Misuse or theft of computer services and operations

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

35

Organisational fraud

SWINBURNE
Slide 36

Data processing

Fraudsters pocket \$10 million in four-year micro-payment scam

29 June 2010 | 11966 views | 1



The Federal Trade
elaborate four-yea
than \$10 million ir
credit and debit ca

At issue are a rash of phony charges levied against countless consumers for odd amounts — such as \$10.37, or \$12.96. When they appear on your statement, the charges generally reference a company in St. Julians, Malta such as BLS*Weblearn or PLI*Weblearn, and include a 1-888 number that may or may not work (the most common being 888-461-2032 and 888-210-6574).

More than a million consumers were hit with one-time charges of \$10 or less, and their payments were routed through 16 dummy corporations in the US to bank accounts in Eastern Europe and Central Asia, alleges the FTC.

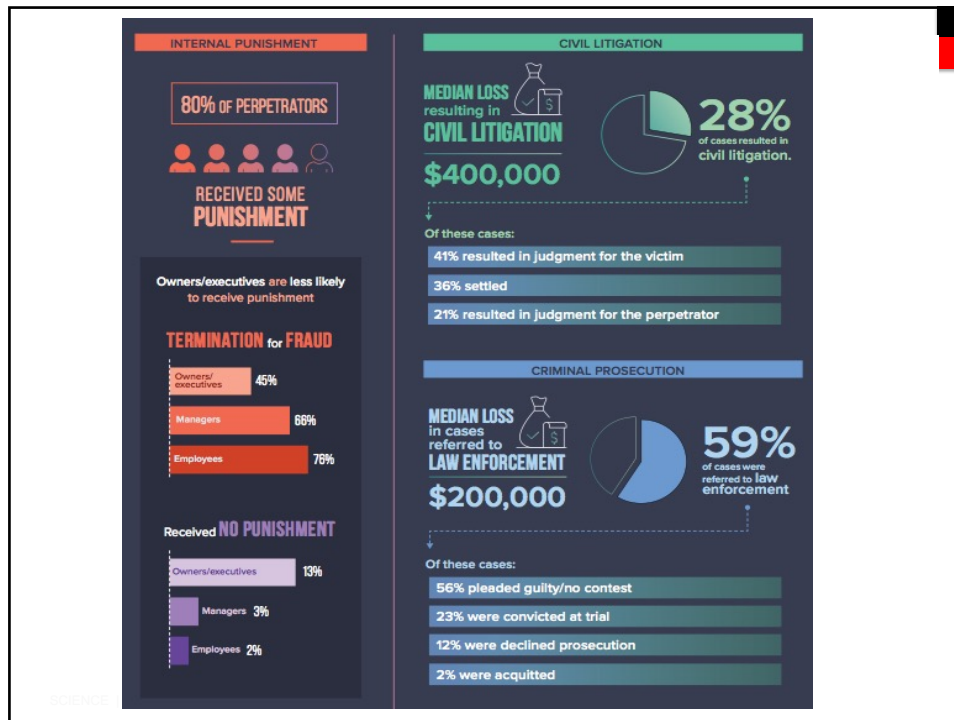
ONLINE LEARNING ACCESS Affiliate Learning System	
PREMIUM WEB TRAINING ACCESS	\$8.83
WEB BUILDING BASICS SIMPLE	\$2.35
PAY PER CLICK	\$2.25
INCREASE YOUR TRAFFIC FLOW	\$1.95
Total:	\$8.83

onlinelearningaccess.com, one of the fraudulent affiliate marketing schemes that powers these bogus micropayments.

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

36



37

Swinburne

Wire fraud: Financial fraud involving the use of telecommunications or information technology (electronic communications or digital networks).

- ✓ 2 counts of conspiracy to commit wire fraud
- ✓ 9 counts of wire fraud

<https://www.youtube.com/watch?v=Y0e778c2Bg0> in 7 minutes

<https://www.youtube.com/watch?v=3CccfnRpPtM> in 24 minutes

OR ABC news youtube and podcast: The Dropout

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

38



39

Organisational fraud

SWINBURNE
Slide 40

Two categories of CAATs

Computer Assisted Audit Techniques (& tools)

1. Approaches to **validate application integrity**
2. Approaches to **verify data integrity**

40

Organisational fraud



Validating application integrity

- Use control testing techniques to provide information about the accuracy and completeness of an application's processes
- **What controls would the auditor be testing?**

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

41

Organisational fraud



Application controls

- Programmed procedures designed to deal with potential exposures that threaten specific applications, such as payroll, purchases, cash disbursement systems
- Three broad categories:
 - **Input** - ensure transactions entering the IS are **valid, accurate & complete**. e.g. source document controls, data coding controls
 - **Processing** - monitor transactions through the processing stage. e.g. Audit Trail Controls
 - **Output** - ensure output is not lost, misdirected or corrupted and that privacy is not violated. report distribution

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

42

Organisational fraud



CAATs to verify data integrity

1. Data extraction and analysis (investigating anomalies in & between records)
2. Fraud detection (detection of anomalies validated by other evidence gathered)
3. Continuous auditing techniques (embedded audit modules and data analytics)

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

43

Thank you

Remember this weeks face
to face class is a group
assignment workshop

SWIN
BUR
NE

SWINBURNE
UNIVERSITY OF
TECHNOLOGY

Swinburne
▶ think forward

44