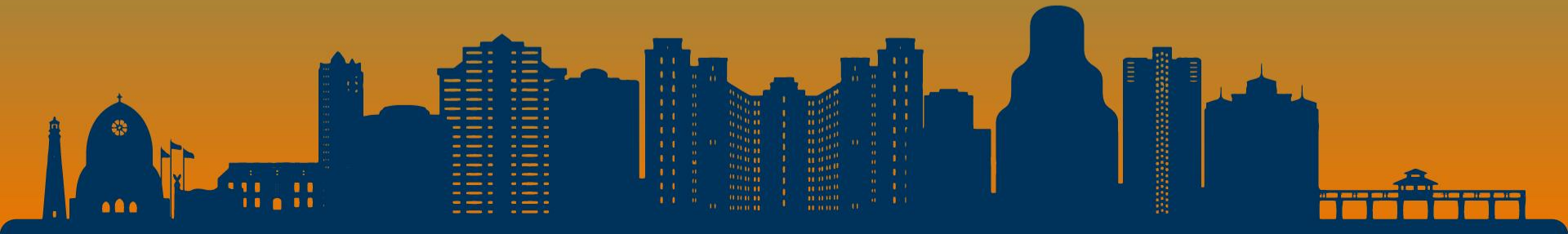
Markus Schuler / CONVISA
19. April 2024 / 11:00am

REIMAGINE NOW

LEA GLOBAL EUROPEAN REGIONAL CONFERENCE



Markus Schuler

Certified public accountant

authorised audit expert

CONVISA

- Switzerland based (german speaking part)
- Full service accounting, audit, legal, tax consulting and advisory firm;
- 3 office locations;
- 50 employees.

Today

- Classic Fraud in Audit
- **AI and Fraud**
- External Fraud affects client
- Cybercrime / going concern / example

Classic fraud in Audit

aspects

- Consideration of fraud is part of the audit planning as well as the audit itself (audit standards)
- Characteristics of fraudulent behaviour:
  - manipulation of the accounting or
  - to misappropriation of assets

Classic fraud in Audit

Manipulation of the accounting

- Recording of **fictitious journal entries**, especially shortly before the balance sheet date, in order to manipulate operational manipulate results or pursue other objectives
- Omitting, bringing forward or deferring the recognition of events and transactions in the financial statements, that during the reporting period have taken place
- Etc.

Classic fraud in Audit

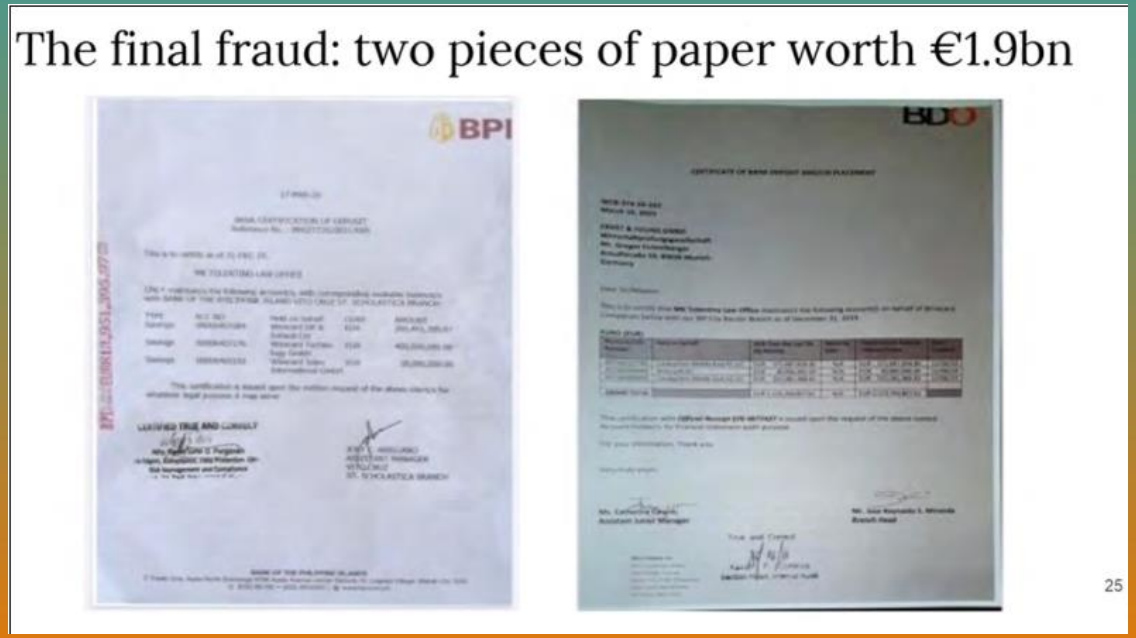
Manipulation of the accounting

- Recording of **fictitious journal entries / example**

Classic fraud in Audit

Manipulation of the accounting

- Recording of **fictitious journal entries / example**



Classic fraud in Audit

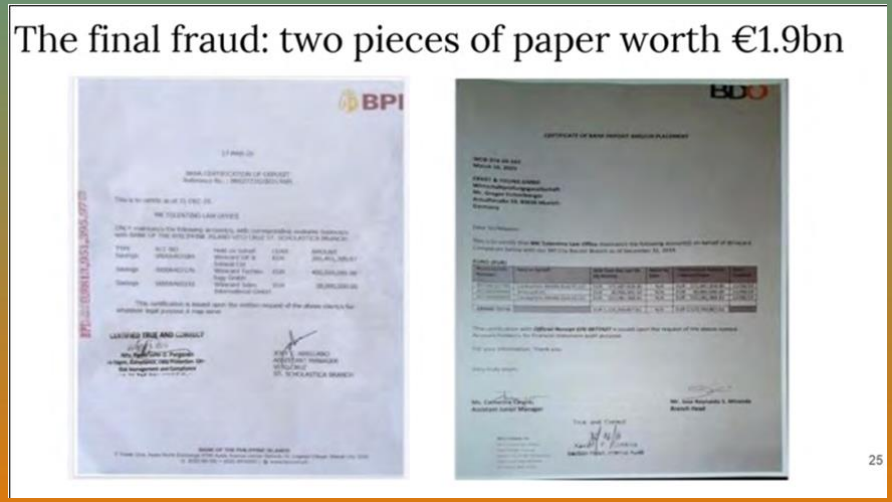
misappropriation of assets

- Misappropriation of payments received
- Theft of assets or intellectual property
- Inducement of payments by the entity for goods and services not received (e.g. payments to fictitious suppliers, "kick-back" payments paid by suppliers to the entity's purchasers in return for inflated purchase prices, or payments to fictitious employees)
- Use of the entity's assets for private purposes (e.g. as collateral for private loans or for loans to related parties).

Classic fraud in Audit

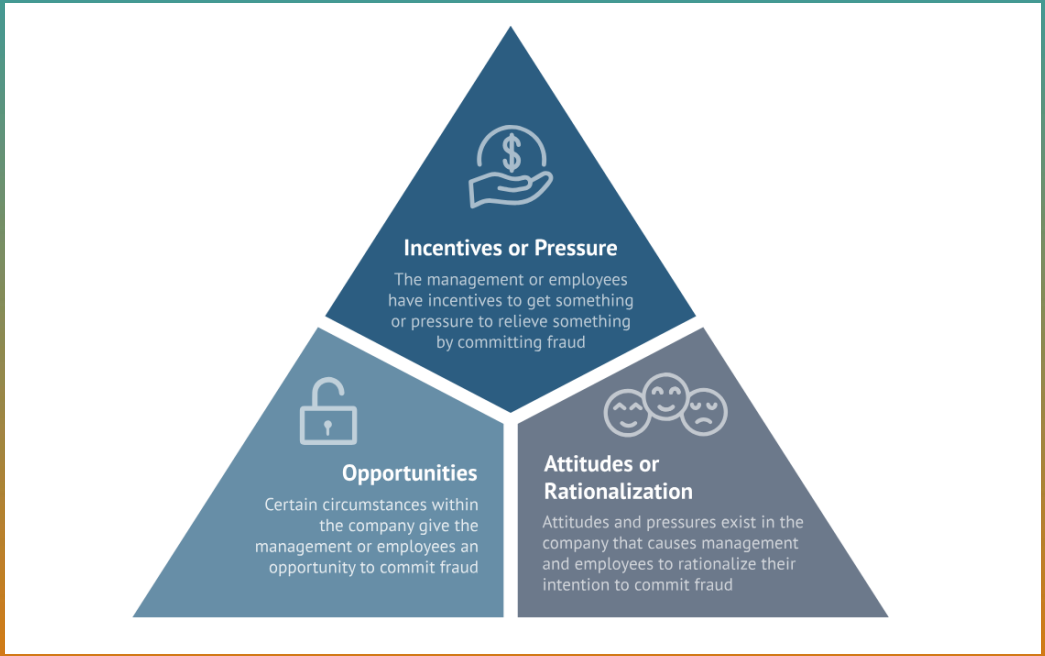
misappropriation of assets

- Misappropriation of asset (theft) often involves false or misleading records or documents designed to conceal the fact that assets are missing or have been pledged without proper authorisation.



Classic fraud in Audit

Fraud triangle / risk assessment



AI and fraud

What's new about

AI and fraud

What's new about

- Generating text and image content by AI
- Deep fakes video
- AI enabled chatbots
- Voice cloning – scams and voice ID
- Sophisticated targeting of victims
- Pressure testing

AI and fraud

What's new about

- Examples

Wegen KI-Kleidung im Videocall aufgeflogen

Bund warnt vor neuer CEO-Betrugsmasche

Schweizer Vereine und Firmen im Visier: Cyberkriminelle setzen künstliche Intelligenz ein, um in Videocalls aufzutreten. So wollen sie Geld ergaunern.

Bei diesem Betrugsfall verschwimmen die Grenzen zwischen Realität und Fiktion: Denn die Cyberkriminellen nutzen die neuesten Technologien, um ihre Opfer zu überrumpeln. Ein solcher Fall wurde jetzt dem Bundesamt für Cybersicherheit (Bacs) gemeldet. Es ist der erste Fall dieser Art in der Schweiz.

In dem filmreifen Szenario wurde ein Finanzchef eines Schweizer Unternehmens von einem Anwalt telefonisch kontaktiert. Dieser lud ihn zu einer Videokonferenz ein. Die Einladung zu dem überraschenden Treffen erfolgte per E-Mail, zusammen mit den Zugangsdaten. Als der Finanzchef der Einladung folgte und sich einwählte, sah er seinen Chef auf dem Bildschirm und begann ein Gespräch mit ihm.

AI and fraud

What's new about

You cannot trust

AI and fraud

What's new about

- Examples from your side?

External fraud affects client

- cybercrime / AI fraud **increased risk**
- Safety of process in general
- IT safety
- employee

External fraud affects client

- increased risk by client means change risk assessment in Audit
- increased risk by client means change risk assessment in consulting and make it necessary to communicate the risk and possible solutions all the time
- increased risk by the customer means a change in our own risk assessment

External fraud affects client

- ……and we must also ensure our own integrity with client

Cybercrime / Going concern

Example

- The Swiss window manufacturer Swisswindows AG was the victim of a ransomware attack with the Ryuk encryption Trojan in May 2019. The company has now filed for bankruptcy on 26 February 2020 and laid off all 170 employees.
  - ERP system down
  - production and all financial cycles stopped
  - end

Q&A

Discussion

Thanks