AAFCPAs

great minds | great hearts

Understanding Your ITGCs

Why They Matter and How to Strengthen Them

November 2025

Thank you for joining us!

Vassilis Kontoglis

Partner, AI Digital Transformation & Security

Lisa Whittemore

CFE, CRMA, MBA | Partner, Risk Advisory

Poll: How confident are you that your organization's IT controls are effective and consistently followed?

A. Very confident
B. Somewhat confident
C. Not confident
D. Unsure

What are IT General Controls (ITGCs) and Why Do They Matter

What You May Be Confronted With:

Surprising Audit Results

Risk Exceptions

Identified Cyber Incident

Regulatory Findings

What's driving these issues?

Lack of compliance

- Poor Data Governance
- Breakdown in controls
- Lack of training, understanding or not following

Emerging risks and blind spots

- Lack of system's inventory
- Web-Based application

Technology advancements

- Social Engineering
- AI

Reduction in budgets / reduced IT spend

- Not being able to keep up with the latest security threats
- Insider threats either by mistake or targeted

Poll: How frequently does your organization conduct formal risk assessments of IT systems?

A. Quarterly or more often
B. Biannually
C. Annually
D. Less than once a year
E. Never
F. Unsure

What's at stake?

- Business continuation
- Reputation
- Financial exposure
- Stakeholder trust
- Sensitive data exposure
- Loss / sale of IP on dark web
- Liability / lawsuits
- Financial loss

Where are your vulnerabilities?

and

Do you know how to identify them?

Do you have:

- A systems inventory list
- IT Security policies and trainings
- Segregation of duties configurations
- Sufficient tone at the top
- IT and cybersecurity risk discussions

Do you perform:

- Regular controls testing
- User access reviews
- Updates and patches
- Monitoring and reporting

Poll: When was the last time your organization conducted a vulnerability assessment on its IT systems?

A. Within the past 6 months
B. Within the past year
C. More than a year ago
D. Never
E. Unsure

Strategic Response: Invest in Strengthening Controls

Strategic Goals:

- **Reduce the risk of fraud and error.**
- **Improve your audit readiness and compliance posture.**
- **Enhance your operational resilience and stakeholder confidence.**

How To's:

1. Assess Current Control Environment
- Perform a risk-based ITGC assessment across key domains
- Identify gaps and control weaknesses impacting financial reporting and operational resilience.

2. Prioritize High-Risk Areas
- Focus on controls that protect critical systems and sensitive data; Support regulatory compliance (SOX, GDPR, HIPAA); Reduce exposure to cyber threats and fraud.
- Use a risk heat map to rank vulnerabilities and allocate resources effectively.

3. Invest in Automation & Continuous Monitoring

4. Embed Governance & Accountability
- Define clear ownership for ITGC processes across IT and business units.
- Establish policies and procedures.
- Create reporting dashboards for visibility.

Investments that yield the greatest risk reduction:

01

Comprehensive Risk Assessment/Heat Map

02

Vulnerability Assessments

03

Cybersecurity Awareness / Phishing Training

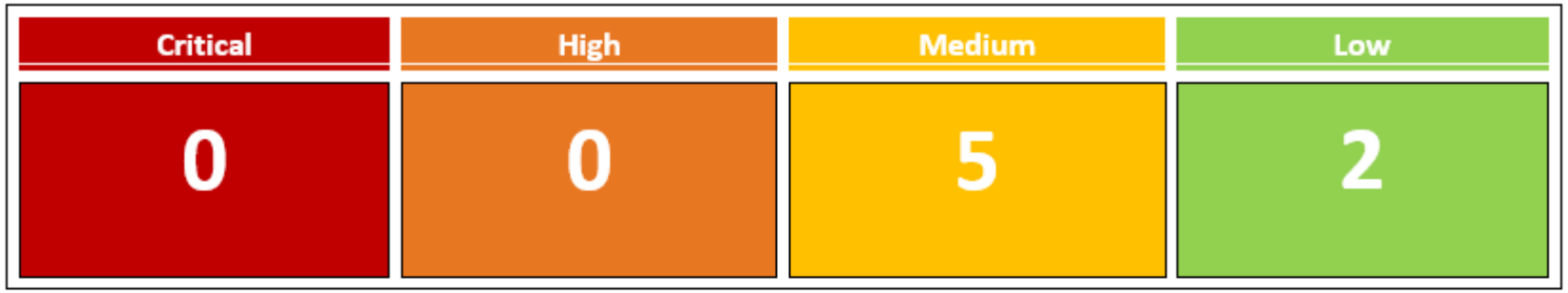
01: Comprehensive risk assessment/heat map

Company XYZ
INFORMATION SECURITY RISK ASSESSMENT
Date

Potential Threat/Damage/Risk	Likelihood (High/Med/Low)	Impact (High/Med/Low)	Initial Risk Level (High/Med/Low)	Company XYZ Control Element/ Information Asset/Mitigating Strategy	Mitigated Likelihood	Mitigated Impact	Mitigated Risk Level (High/Mod/Low)	Comments/Results	Future Risk Mitigation
Unauthorized Access to LAN/WAN	Medium	High	High	• Unused ports located in public spaces are disconnected from any switch • Data closets are secured • Guest WLAN and corporate LAN is logically separated • Routine scan of network to reveal rogue devices • Unauthorized user detection through the use of a SIEM	Low	Medium	Low	Residual risk • Connecting to a port where a device is already attached • After hours wireless password cracking attempts	Port Security • Enabled ports should only allow for s MAC addresses to be connected to e • If an unauthorized device is connecte port, the port should automatically shu the IT department should be notified • Enabling IP source guard (part of por will mitigate the effects of IP address s attacks on the Ethernet LAN • WLAN isolated to separate firewall r
Confidential information (member, employee, corporate, etc.) transmitted electronically (ftp, email, etc.) may be intercepted.	Medium	Medium	Medium	• User initiated email encryption • Secure file sharing services in use • All eCommerce connectivity is encrypted.	Low	Low	Low	Residual risk • Employee fails to encrypt email message • Insider threat – employee sends account and/or SSNs to an external email address	Implement automated data leak protec
Improper storage or loss of computer media containing confidential information.	Low	High	Medium	• Procedures exist covering storage of confidential information. • Backup tapes are encrypted • External storage device usage is disabled by default • Physical access to backup media stored in the server room is restricted and monitored • Video monitoring in place • Any confidential informaiton stored on portable media is encrypted	Low	Low	Low		Researching options for an electronic solution at the DR site. Inventory procedures need to be creat physical media that is kept in the data • Member data at rest is encrypted
Inappropriate computer use leading to lack of productivity, malware, etc.	Medium	High	High	• Firewall is installed on Company XYZ perimeter o Filters inappropriate websites o Blocks inappropriate web adds • Centrally managed Antivirus is enabled and installed on every computer • Intrusion Detection System is installed with auto notification enabled • Employees are trained on information security best practices (New Hire orientation, existing employee annual) •Adminstrator privilege is restricted to appropriate personnel	Low	Low	Low	Residual Risk: • Employees may not adhere to the guidelines • 0-Day viruses • Lack of oversight on employee computer usage	

02: Vulnerability Assessments

The cumulative total number of vulnerabilities is as follows:



Hosts Executive Summary

In the following Executive Summary, vulnerabilities are listed as total unique vulnerabilities per host listed by severity. In some instances, the same vulnerability may be found on multiple protocols or ports but may be listed as a single vulnerability. In the detailed attachment, the protocols/ports per host are listed individually.

Host	Critical	High	Medium	Low	Total
#.#.#.#			5	2	7
GRAND TOTAL	0	0	5	2	7

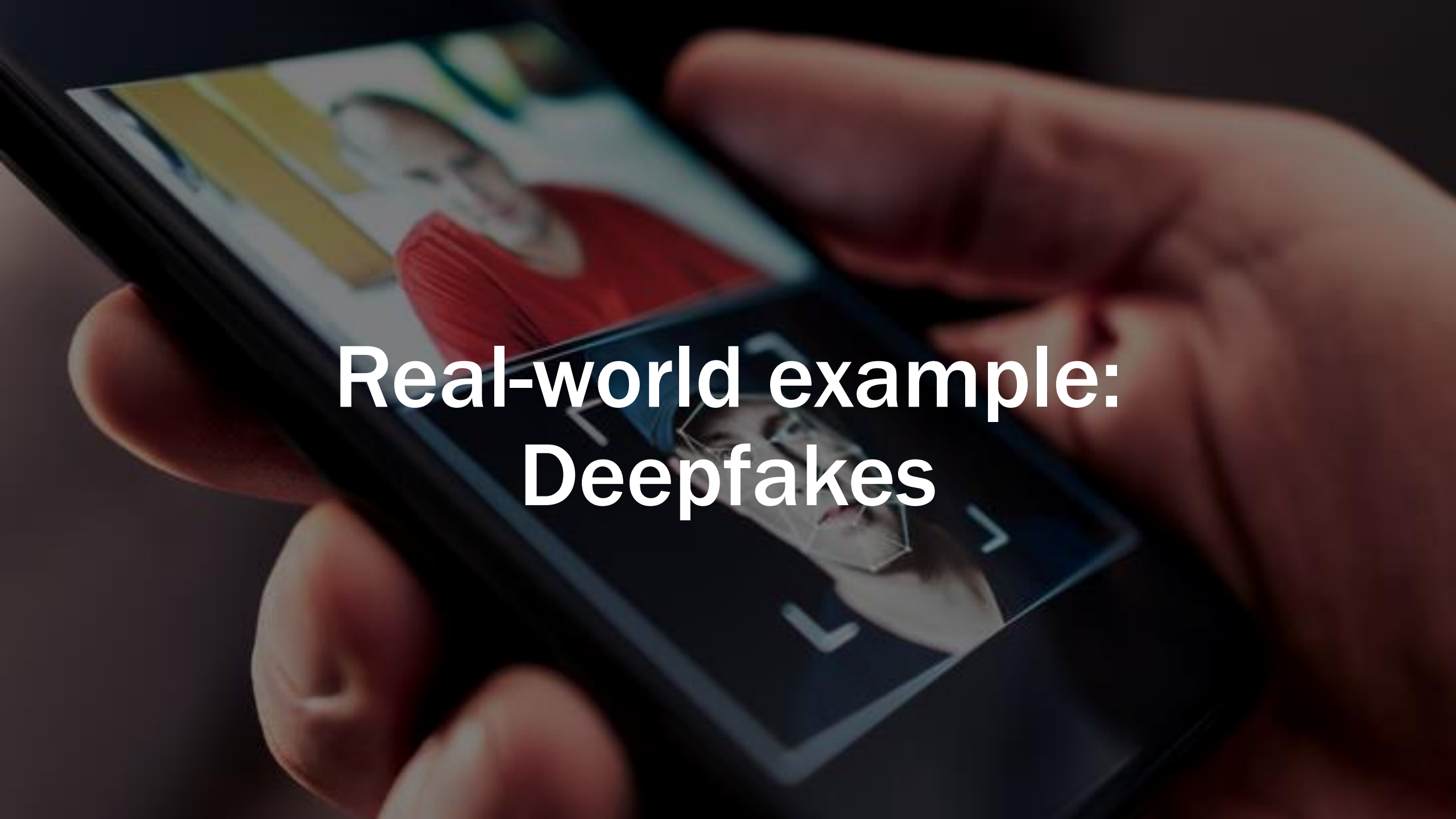
03: Cybersecurity awareness / phishing training

Poll: Does your organization provide annual cybersecurity training to all employees?

A. Yes, every year
B. Occasionally (not every year)
C. No, never
D. Unsure

Real-world example: Web based access

Real-world example: Social Engineering

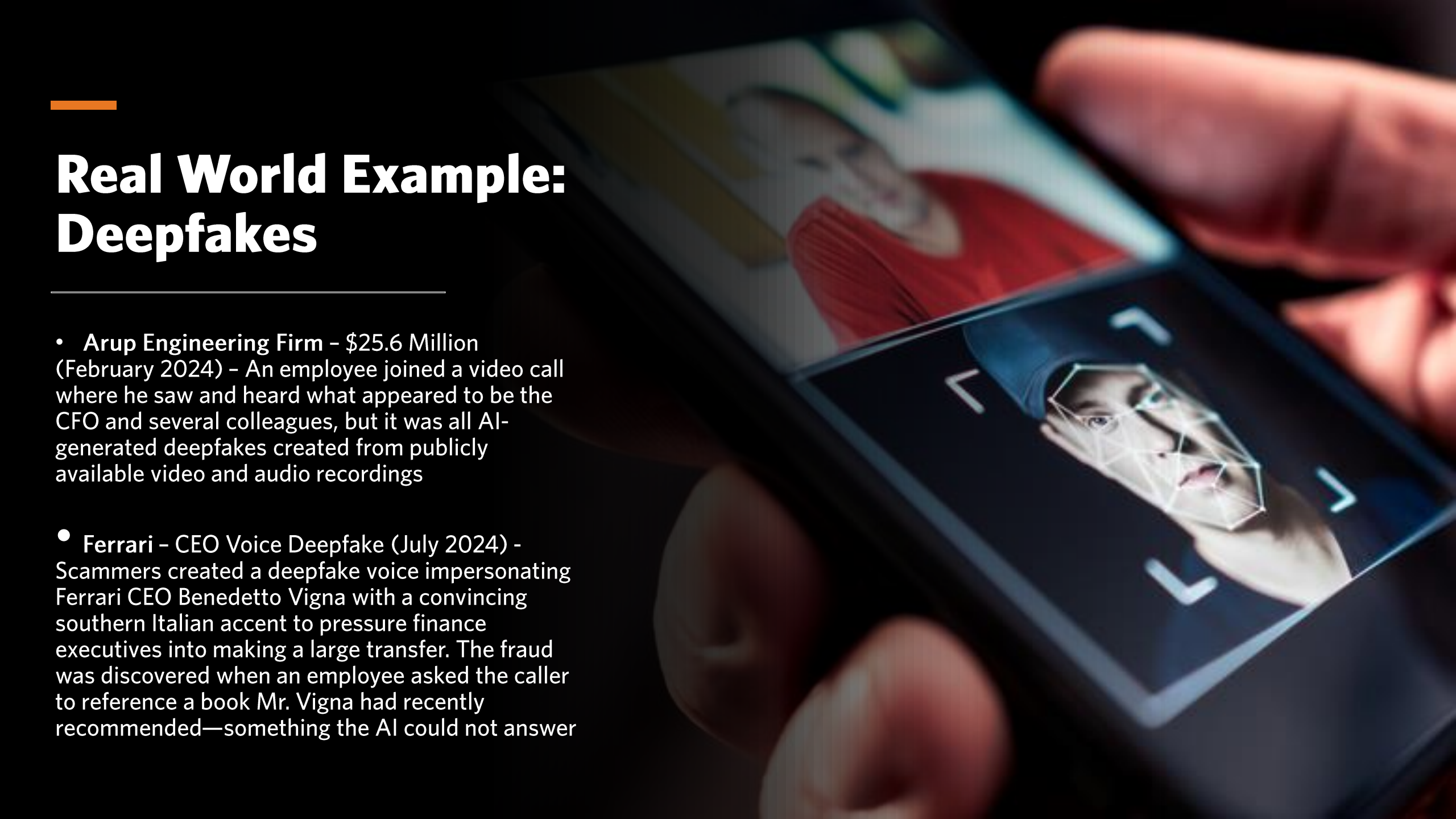


Real-world example: Deepfakes

Real World Example: Deepfakes

- **Arup Engineering Firm** – $25.6 Million (February 2024) – An employee joined a video call where he saw and heard what appeared to be the CFO and several colleagues, but it was all AI-generated deepfakes created from publicly available video and audio recordings

- **Ferrari** – CEO Voice Deepfake (July 2024) - Scammers created a deepfake voice impersonating Ferrari CEO Benedetto Vigna with a convincing southern Italian accent to pressure finance executives into making a large transfer. The fraud was discovered when an employee asked the caller to reference a book Mr. Vigna had recently recommended—something the AI could not answer



How we help:

Risk Assessment And Prioritization

Control Design And Implementation

Ongoing Monitoring And Reporting

AAFCPAs
great minds | great hearts

Questions?

Vassilis Kontoglis	774.512.4069	vkontoglis@aafcpa.com
Lisa Whittemore, CFE, CRMA, MBA	774.512.4116	lwhittemore@aafcpa.com

The information in this presentation is intended to be general guidance and should not be considered legal, accounting, or tax advice. Recommendations are not one-size-fits-all—your organization's unique situation may require different approaches or specialized input. Before making decisions or taking action based on this material, please consult your AAFCPAs advisor. Keep in mind, future changes or new developments could also impact the relevance of this information.

AAFCPAs
great minds | great hearts