Pulling fraud out of the shadows

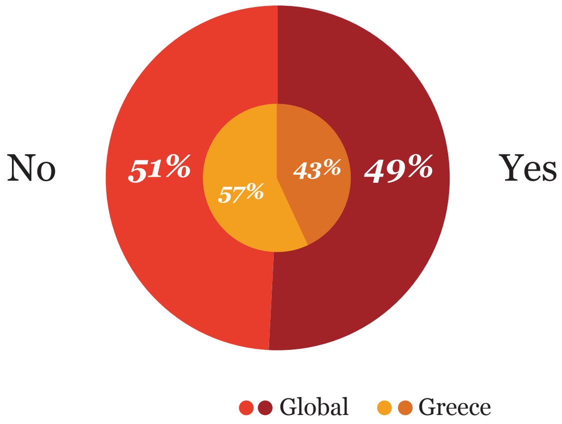
2018 Global Economic Crime and Fraud Survey Highlights

Greece insights

Overview

43%

of Greek respondents vs **49%** globally experienced fraud and/or economic crime



Most common types of fraud and economic crime

Asset misappropriation
45%
(GR 50%)*

Cybercrime
31%
(GR 35%)*

Fraud committed by the consumer
29%
(GR 50%)*

Perpetrators

52% globally ***(GR* 45%)*** of fraud was committed by ***internal*** actors

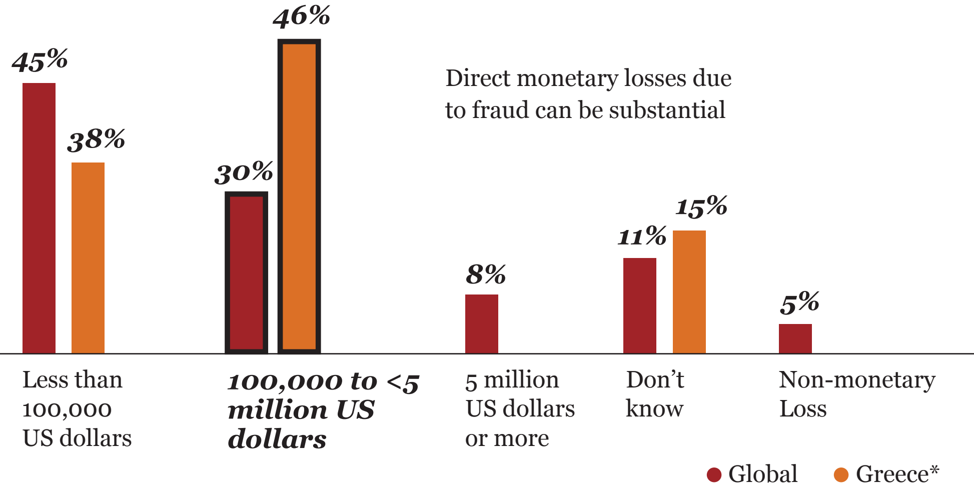
Greece lags in the perception about the impact of fraud or economic crime

Global	52% Employee Morale	38% Business Relations	36% Reputation
*Greece**	27% Employee Morale	12% Business Relations	8% Reputation

Answers: High to medium impact

Losses

Direct monetary losses due to fraud can be substantial



4 steps to fight fraud

1. Recognise fraud

This year, **43%** of Greek respondents said their companies had suffered fraud in the last two years. The gap between the reported fraud globally **(49%)**, may indicate a lower level of fraud awareness, a greater perception about the effectiveness of the anti-fraud systems and controls, or a more limited ability to detect fraud. Organisations are **vulnerable to blind spots**, which usually become apparent only after an incident. ***Throwing light*** promptly can ***open up opportunities*** for big improvements in the fraud-fighting efforts.

Just over half of the most disruptive frauds were detected by corporate controls

Corporate controls[1]
52%
(GR* 55%)

Corporate culture[2]
27%
(GR* 30%)

Beyond the influence of Management[3]
14%
(GR* 10%)

1. Internal audit, fraud risk management, suspicious activity monitoring, corporate security, data anlytics, rotation of personnel
2. Tip-off (internal or external), whistleblowing hotline
3. By accident, by law enforcement, investigative media

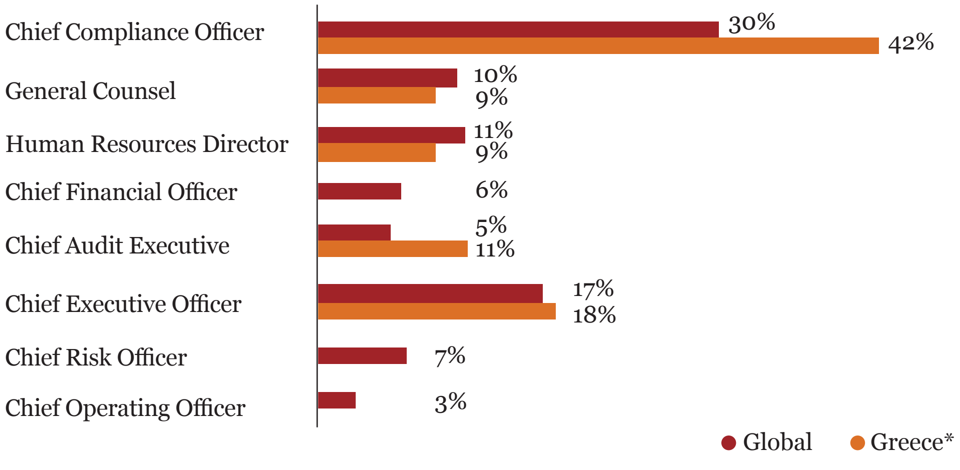
● Global ● Greece*

2. Take a dynamic approach

By preventing fraud and economic crime you save not only on fraud losses but also on secondary costs. ***34%*** of Greek respondents said that their organisation spent the ***same or more on investigations*** and other interventions than was directly lost to fraud itself. The ***public's tolerance*** for corporate and personal misbehaviour is declining – fast.

This, emphasises the ***role of the C-suite***, as what it does to ***prevent*** or ***deal with*** a crisis has a high likelihood of becoming a measure by which it will be judged.

Primary accountability for ethics and compliance programmes resides with the C-suite



3. Harness the protective power of technology

Only ***8% of the Greek* respondents*** vs ***15%*** globally declared cybercrime to be the most disruptive experienced crime in the past two years, while for the next two the perception is ***27%*** and ***26%*** respectively.

When it comes to fraud, ***technology is a double-edged sword. Cybercrime*** is not a stand-alone offence but rather ***a means*** to commit other types of fraud. On the fraud ***defence*** front, organisations can now call on a wealth of ***innovative technologies*** like predictive analytics, machine learning and other artificial intelligence techniques. The good news is they're starting to use them – but there's still some way to go to harness their full potential.

Cybercrime techniques & impact

Cyber-attack techniques
Phishing: ***33%, (GR 44%)***
Malware: ***36%, (GR 41%)***

Impact
Business Process Disruption: ***30%, (GR* 43%)***
Asset Misappropriation: ***24%, (GR* 30%)***

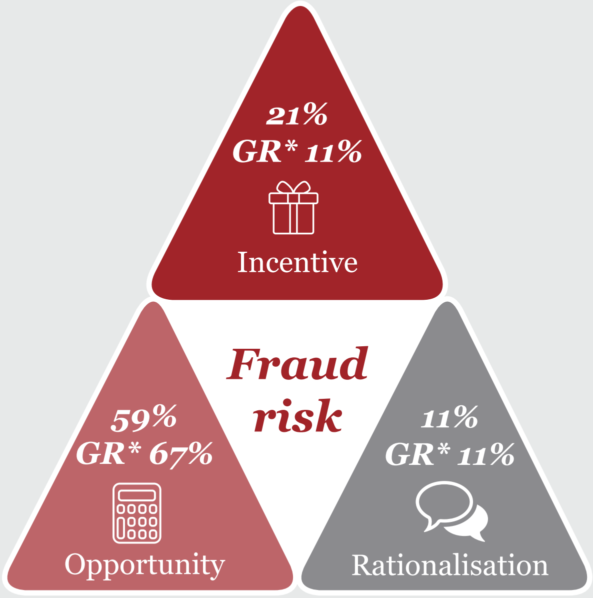
4. Invest in people

Faced with rising fraud risks, many organisations decide to pour more money into technology. Yet when it comes to fighting fraud – especially internal fraud – technology investments can reach a point of diminishing returns.

Fraud is the product of a complex mix of conditions and motivations, only some of which can be tackled by machines.

When it comes to blocking that 'last mile' to fraud, ***the returns from people initiatives*** are likely to far exceed those from investing in another piece of technology.

The fraud triangle: what makes an employee commit fraud?



Are you prepared?

1. Identify Fraud

Have you completed a **fraud risk assessment** recently?

Is your **fraud programme** organisation **- wide or siloed?**

Do you **share** alerts and findings on fraud **across** your entire organisation?

Do you **test** your internal controls to determine if they **work effectively?**

---

2. Dynamic Approach

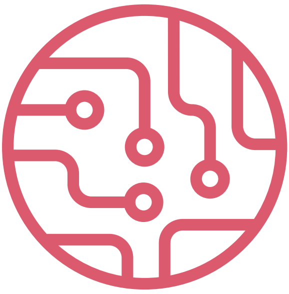
Do you have a **crisis response plan?**

Have you **demonstrated** a plan to **all** the appropriate **stakeholders?**

What **compliance exercise** have you done to **test** your organisation's ability to **manage** the crisis?

---

3. Technology



Are you **evaluating** where **technology** can **replace** old processes?

Is technology an **instrumental** part of your **fraud monitoring** activities?

Have you considered using **your fraud monitoring technology** not just reactively but **predictively?**

---

4. People

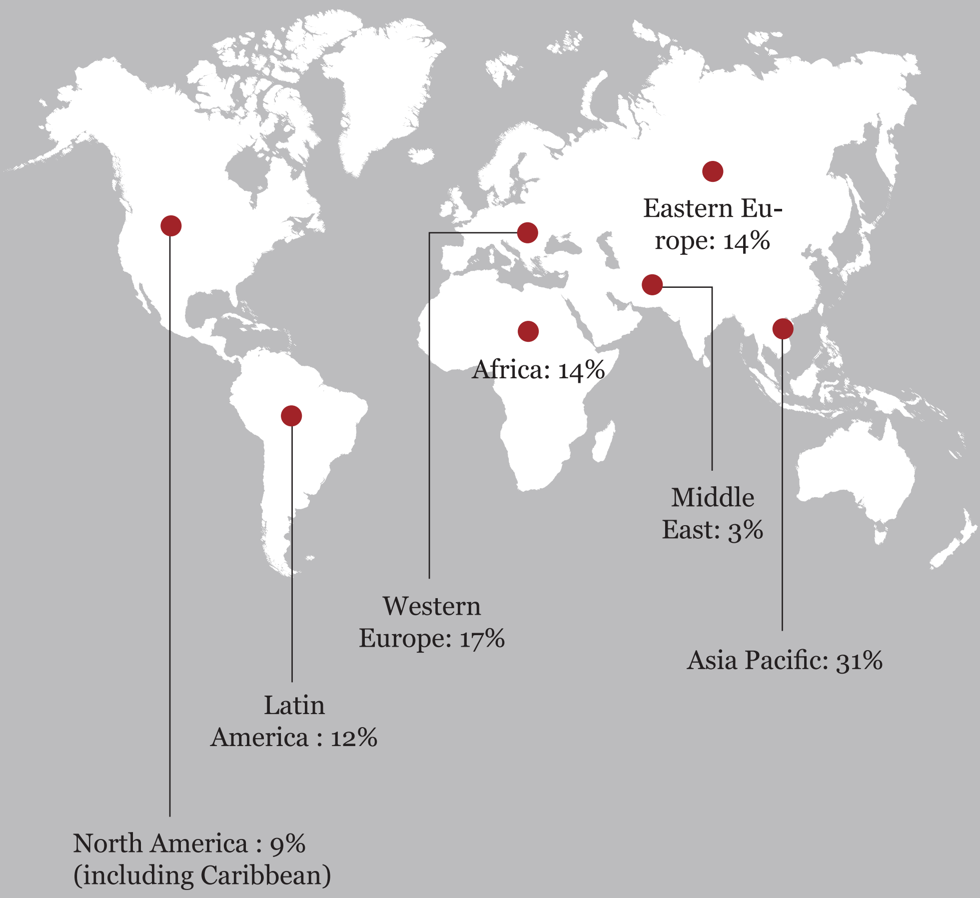
Do you know the **norms** for ethics and compliance in your industry?

Does your **ethics and compliance** programme explicitly target fraud?

Does your **incentive** programme consider **pressures** that it can create on your employees and can you **monitor** it?

Do you have an **open-door policy** or hotline that could serve as an **early warning sign** of internal fraud?

>7,200 respondents
Across 123 countries
61 respondents in Greece



*Conclusions are indicative due to respondents’ population size

Contacts

Kostas Perris
Partner
+30 210 687 4002
kostas.perris@gr.pwc.com

Michalis Pikis
Director
+30 210 687 4071
michalis.pikis@gr.pwc.com