AlixPartners

AGiG ACCOUNTANTS GROUP in GERMANY

Cracking fraud
Practical insights and prevention strategies

91st AGIG seminar

13 November 2025 | Novotel Frankfurt City

Marie-Christine Döscher

mdoescher@alixpartners.com

+49 152 22401687

AlixPartners

Agenda

01	From internal issue to public scandal
02	Fraud – Definition, importance, risk
03	Psychology of misconduct – The Fraud Diamond as an analytical model
04	Trust through structure – How organizations prevent fraud
05	Focus – Risk analysis
06	Future outlook – Compliance under pressure

From internal issue to public scandal

01

AlixPartners

From internal issue to public scandal

Kriminelle räumen Konten von Commerzbank-Kunden leer

Bei Deutschlands zweitgrößter Privatbank haben Unbekannte offenbar von mehr als 100 Konten einen zweistelligen Millionen-Betrag abgebucht. Sie sollen Girocards mit einer bestimmten Funktion genutzt haben.

Finanzaufsicht greift bei Volksbank Düsseldorf durch

Datenleck trifft mehr Kunden von ING und Deutscher Bank als bislang bekannt

Nach einem Angriff auf den Kontowechsel-Dienstleister Majorel sind nun Kundennamen und IBANs im Darknet veröffentlicht worden. Bei den Banken wächst der Unmut.

Wird der Bank-Verlag den Karten-GAU bei der Commerzbank überleben?

„Unterirdisch“ - Kreditkartenbetrug bei ADAC-Partner Solaris-Bank schlägt weiter Wellen

Fraud – Definition, importance, risk

02

AlixPartners

Fraud – Definition, importance, risk

Definition

A deliberate act by one or more individuals, members of the management responsible for directing and overseeing an organization, other employees, or third parties, intended to obtain an unjustified or unlawful financial benefit to the detriment of the organization.

Internal fraud

Behavior committed by individuals within the organization, typically employees, executives, or others with privileged access to systems and information.

Examples

- **Embezzlement:** An employee diverts client funds to personal accounts.
- **Loan approval manipulation:** A client advisor grants loans to straw men or in exchange for kickbacks.
- **Expense fraud:** False or inflated claims for business travel expenses.
- **Salary or bonus fraud:** Unauthorized approval of bonuses or salary increases through system manipulation.

External fraud

Activities carried out by individuals outside the organization, such as customers, suppliers, cybercriminals, or organized crime groups.

Examples

- **Phishing:** Customers or employees are tricked into disclosing access credentials.
- **Identity theft:** Opening accounts under a false name.
- **Credit card fraud:** Use of stolen or counterfeit cards.
- **Trade-based money laundering:** Using trade transactions to disguise illicit funds.

The global cost of fraud – An overview

1,921 CASES from **138** COUNTRIES and TERRITORIES

Causing total losses of more than **$3.1 BILLION**

$1,662,000
Average loss per case

22% of cases had losses of $1 million+

CFEs estimate that organizations **LOSE**

5% of revenue to **FRAUD** each year

Projected against 2022 GWP*
($101 TRILLION)

that's more than
$5 TRILLION LOST TO FRAUD GLOBALLY

*https://databank.worldbank.org/data/download/GDP.pdf

Source: Occupational Fraud 2024: A Report to the Nations

Fraudulent schemes – Umasking the damage

ASSET MISAPPROPRIATION SCHEMES
are the most common but least costly

89% of cases

$120,000 median loss

FINANCIAL STATEMENT FRAUDS
are the least common but most costly

5% of cases

$766,000 median loss

48%

CORRUPTION
Almost half of all reported cases included corruption

ACFE Association of Certified Fraud Examiners

Source: Occupational Fraud 2024: A Report to the Nations

AlixPartners

Psychology of misconduct – The Fraud Diamond as an analytical model

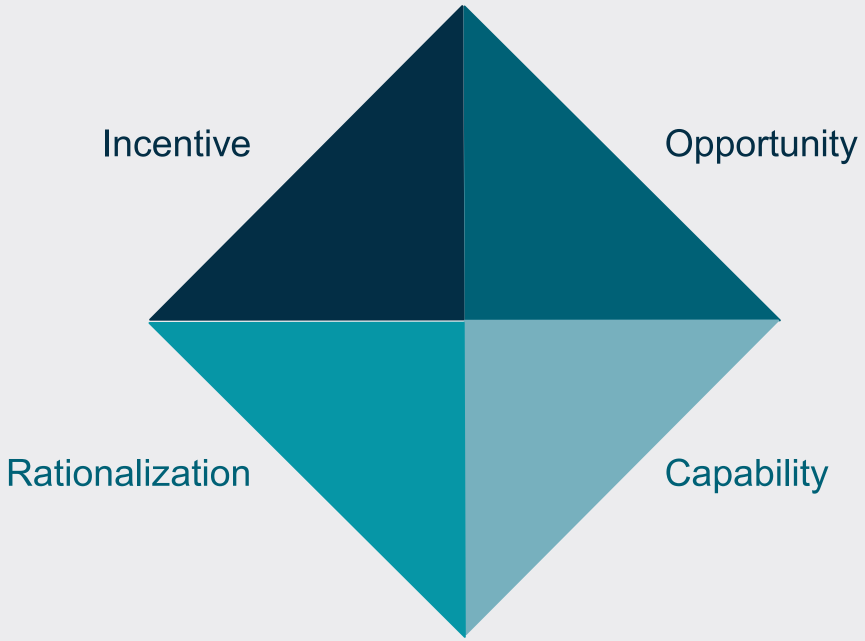
03

Psychology of misconduct – The Fraud Diamond as an analytical model

The Fraud Diamond

- Model for explaining and analyzing fraudulent activities.
- Builds on the earlier Fraud Triangle developed by Donald R. Cressey.

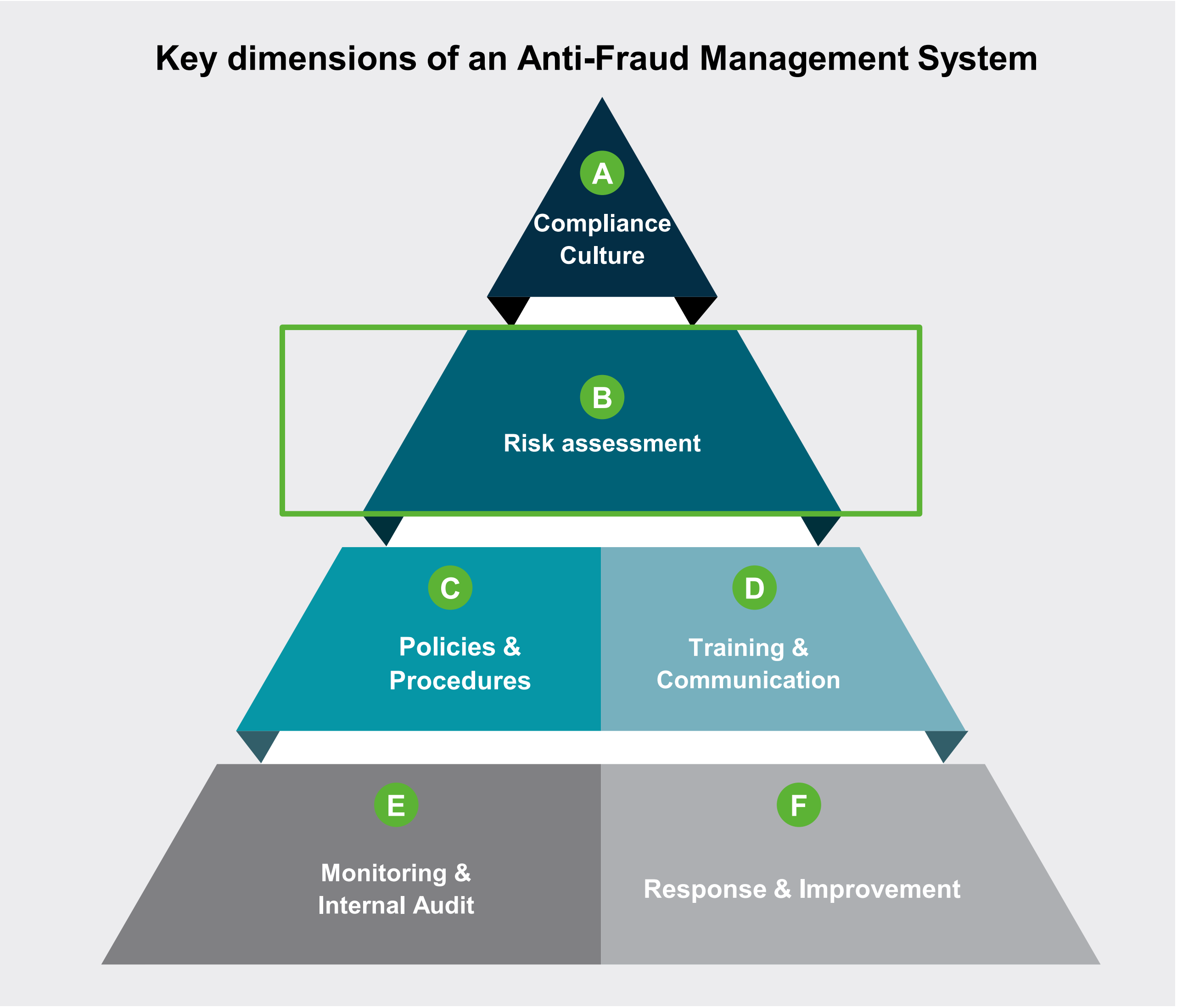
1. Motivation/Incentive
2. Opportunity (Weaknesses in the control system)
3. Rationalization (the internal justification of the act by the perpetrator)
4. Capability (the perpetrator’s ability to carry out the act)



Trust through structure – How organizations prevent fraud

04

Trust through structure – How organizations prevent fraud



A
- Evaluate leadership commitment to ethical conduct ("Tone from the Top")
- Assess alignment between stated values and actual business behavior
- Review governance structures and accountability mechanisms

B
- Identify sector-specific, geographic, and third-party compliance risks
- Review historical incidents, investigations, or regulatory findings
- Analyze risk management processes and documentation

C
- Verify the existence and accessibility of key fraud-related policies (e.g., anti-corruption, data protection, antitrust)
- Assess implementation and enforcement mechanisms
- Monitor regular updates and legal compliance

D
- Review training records and participation rates across functions
- Evaluate awareness levels and understanding of compliance topics
- Assess internal communication channels and messaging consistency

E
- Examine internal control systems and audit reports
- Review KPIs and dashboards used for compliance monitoring
- Assess effectiveness of whistleblower systems and reporting mechanisms

F
- Analyze procedures for handling violations and conducting investigations
- Review documentation of remediation actions and disciplinary measures
- Evaluate mechanisms for continuous improvement and feedback loops

Focus – Risk analysis

05

Risk analysis as the foundation of effective fraud prevention

What is a risk analysis and what is its purpose?

- A risk analysis is a central, systematic process that enables organizations to identify, assess, and prioritize risks arising from non-compliance with laws, regulations, or internal policies. It provides transparency regarding potential vulnerabilities and supports the development of preventive measures as well as the review of existing safeguards and controls. Beyond identifying and prioritizing areas for action, it also raises awareness among all stakeholders about relevant compliance issues.
- The objective is to strengthen the compliance organization effectively. As a dynamic and ongoing process, it should continuously adapt to emerging risks and changes. Furthermore, risk analysis contributes to protecting the organization's reputation by demonstrating that risks are systematically addressed and managed responsibly.

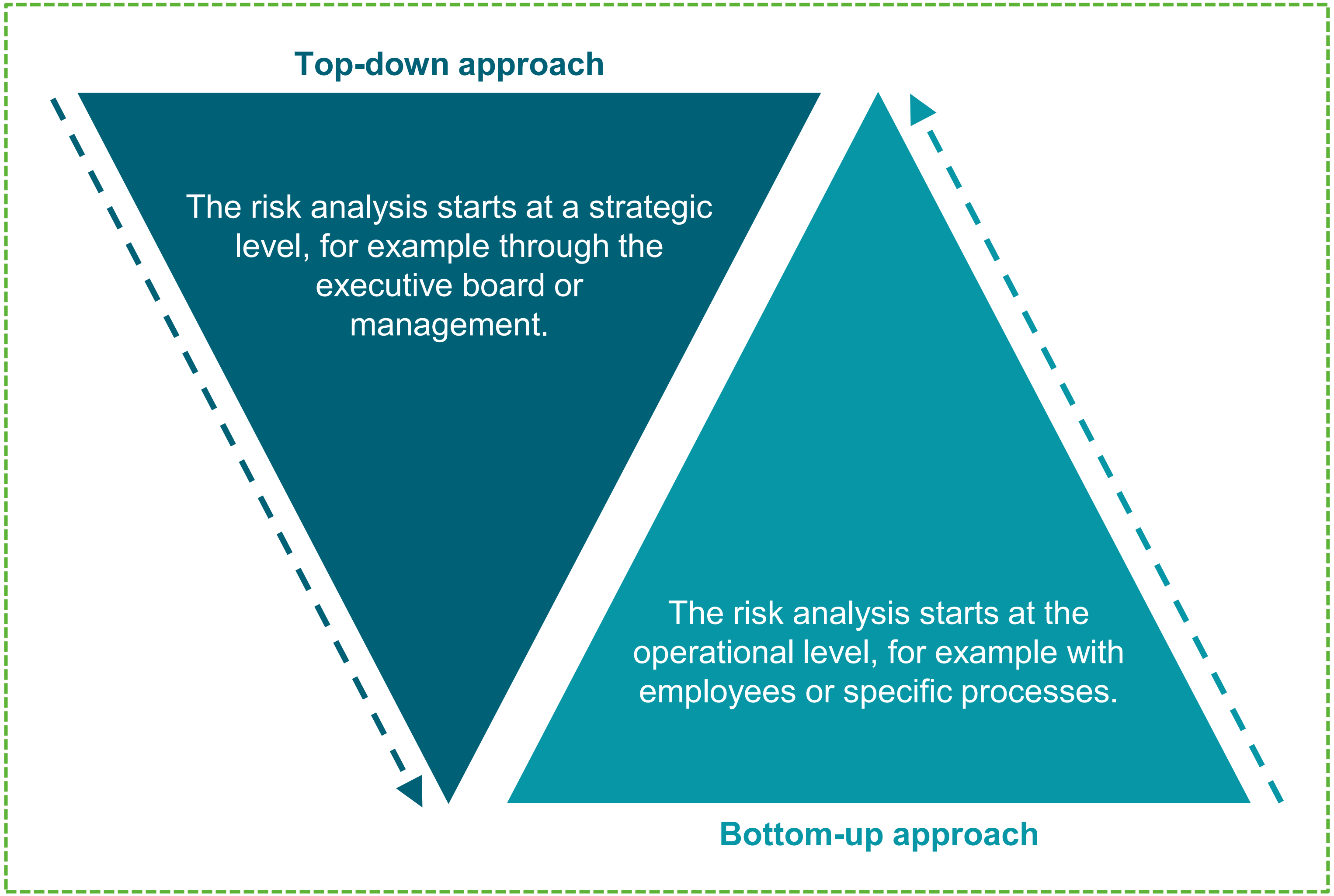
Conducting a fraud risk analysis

Key principles

A risk analysis represents a combination of **strategic approach and practical implementation**.

First, the relevant risk areas are defined from a **strategic perspective**. Subsequently, specific risk scenarios are derived in **workshops with subject matter experts**.

Building on this, **standardized questionnaires are developed** to identify and assess risks, which are then completed by the relevant stakeholders.



Conducting a fraud risk analysis

Methodology of risk analysis

Data basis

Qualitativ

Qualitative assessment of risk factors and controls through questionnaires and workshops

Quantitativ

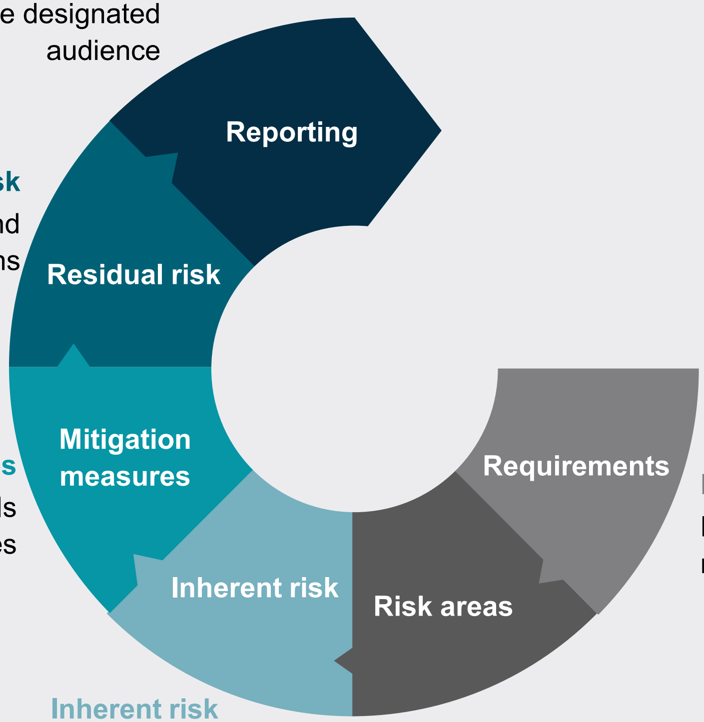
Quantitative assessment of risk factors and controls using business and compliance data

Risk analysis

Result and reporting
Report to the designated audience

Residual risk
Determin residual risk and follow-up actions

Mitigation measures
Assess existing controls and protective measures



Define requirements
Methodological requirements regarding content and scope

Inherent risk
Assess inherent risk based on the information provided in the questionnaires (regarding relevant risk areas/risks)

Risk areas
Identify and define relevant risk areas and scenarios

Results and reporting

Reporting

Create a risk profile

Follow-up actions

Derive additional measures for risk mitigation

Framework for risk assessment

01

Record & identify potential risk scenarios

- The Compliance function has identified potential risks and derived corresponding risk scenarios.

Result

- Overview of potential risks and derived risk scenarios

02

Assess relevance & evaluate gross risk

- The business units perform a relevance assessment.
- Subsequently, a risk evaluation is conducted based on the factors 'Financial Risk', 'Reputational Risk', and the potential likelihood of occurrence.

Result

- Selection of relevant risks and calculated gross risk for each applicable area

Low	Moderate	High

03

Mitigation measures

- Implemented mitigation measures that reduce the gross risk of the respective risks are documented.
- Mitigation measures are assigned to relevant risks.
- The effectiveness of mitigation measures is evaluated.

Result

- Assessment of mitigation measures based on their effectiveness (i.e., impact on the risk)

High effectiveness

Moderate effectiveness

Low effectiveness

04

Determination of net risk

- Net risk is determined by taking into account the effectiveness of mitigation measures.

Result

- Overview of residual risks by relevant area and risk category

Low	Moderate	High

05

Required actions

- Each calculated net risk must be assigned an approach for handling and any resulting required actions.

Result

- Overview of how each net risk is addressed

Avoid the risk

Accept the risk

Mitigate the risk

Transfer/Insure the risk

Outline of risk analysis – A consolidated overview

I. Contextual framework

1. Background and objective
2. Risk analysis within AFMS
3. Methodology
4. Responsibilities
5. Scope

II. Framework conditions

1. Gross risks by risk category
2. Mitigation measures
3. Net risks by risk category

III. Recommended actions

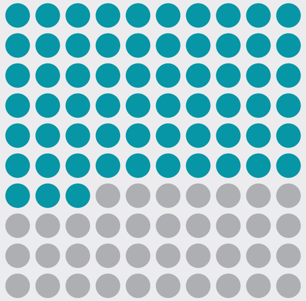
1. Overview of the results
2. Derived (primary) need for action
3. Next steps

Future outlook – Compliance under pressure

06

Future outlook: Compliance under pressure

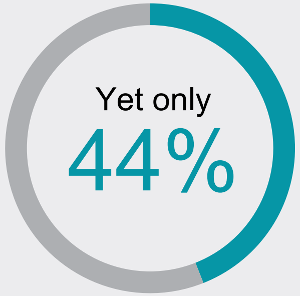
Financial crime



63%

believe financial crime will increase in the next 12 months.

>60% are investing in technology to combat it.

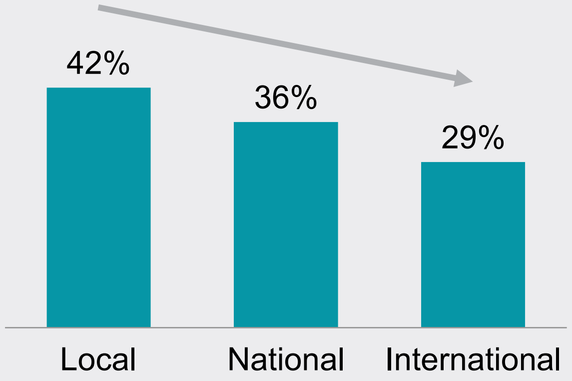


say their technology is very effective at detecting and analyzing risk factors.

Regulatory

Fewer than half of respondents feel very prepared to adapt to potential regulatory changes

.



With the sanctions landscape in flux, only about a third of responders feel very prepared to respond to potential changes.

Technology

Fewer than 40% say their organizations are very prepared to address cybersecurity incidents, data privacy breaches, and digital disruption.

93%

of organizations are implementing AI into their business functions.

~50%

But nearly half do not have an AI lead or AI policies and guidance in place.

Litigation

Nearly 70% believe corporate litigation will increase in 2025.

Of those respondents, about

6 von 10

plan to raise their budget

and/oder

increase their engagement with outside counsel.

Source: AlixPartners 2025 Global Risk Survey

AlixPartners


AlixPartners