



Good Governance – damit der Fisch nicht am Kopf anfängt zu stinken
62. Fachveranstaltung Netzwerk Risikomanagement vom 13. November 2024



1. Good Governance in der Theorie
2. Good Governance in der Praxis
3. Täter und Gründe für Wirtschaftskriminalität
4. Prävention: Unternehmenskultur
5. Werkzeuge
6. Interne Untersuchung
7. Key Take aways / Food for thought

01

Good Governance in der Theorie



Good Governance

Ein Überblick

Governance in OrgR regeln.

Generalversammlung

- Der Generalversammlung als oberstes Organ einer Aktiengesellschaft (OR 698 Abs. 1) obliegt die unübertragbare Befugnis, die Jahresrechnung zu genehmigen (OR 698 Abs. 2 Ziff. 4).
- Demgegenüber sind insbesondere die Oberleitung der Gesellschaft, die Festlegung der Organisation und die Ausgestaltung des Rechnungswesens gemäss OR 716a Abs. 1 unübertragbare Aufgaben des Verwaltungsrats.
- Die **Generalversammlung ist nicht befugt, über die Ausgestaltung des IKS zu befinden** (Pfaff, D., Ruud, F. (2020). Schweizer Leitfaden zum Internen Kontrollsystem (IKS) (8. Auflage), S. 54).
- **Dennoch sind die Aktionäre sehr daran interessiert, dass ein effektives Risikomanagement und ein gut funktionierendes IKS vorhanden sind.**

Verwaltungsrat

- Der VR ist gemäss OR 716a Abs. 1 Ziff. 5 in der Verantwortung, die mit der Geschäftsführung betrauten Personen im Hinblick auf **Einhaltung von Gesetz, Statuten, Reglementen und Weisungen zu überwachen**.
- Das bedeutet, dass die aus der Risikoidentifikation ermittelten Risiken entsprechend zu reglementieren und die Einhaltung der Reglemente zu überwachen sind.
- Zur Unterstützung der Wahrnehmung seiner Aufgaben betreffend dem IKS kann der Verwaltungsrat aus **seiner Mitte einen Ausschuss einsetzen** (z.B. ein «**Audit Committee**» oder ein «**Risk Committee**»).

Geschäftsleitung

- Die GL ist für die Umsetzung der Vorgaben des VR sowie das Erfüllen von dessen **Anforderungen bezüglich Ausgestaltung und Aufrechterhaltung des IKS zuständig**, sofern diese Aufgaben nicht vom Verwaltungsrat selbst wahrgenommen werden (Art. 716b OR).
- Gemäss PS-CH 890 beinhaltet dies u.a. folgende Aufgaben (EXPERT-suisse, 2022. PS-CH 890 III Bst. e.):
 - Entwicklung geeigneter Prozesse zur Identifikation,
 - Einschätzung und Überwachung der eingegangenen Risiken;
- Zudem stellt die GL die **ausreichenden personellen Ressourcen und Mittel** mit der **entsprechenden Qualität hinsichtlich Ausbildung und Erfahrung zur Verfügung**.

Good Governance

Three lines of defense Model

Das Modell der drei Verteidigungslinien, das 2013 vom Institute of Internal Auditors (IIA) veröffentlicht wurde, hat sich international als Konzept zur organisatorischen Einbettung der Kontrollfunktion etabliert. Es beschreibt, wie das Risiko durch drei sogenannte Verteidigungslinien auf das vom VR akzeptierte Restrisiko reduziert wird.

Erste Verteidigungslinie:

Die operativen Einheiten bzw. das operative Management sind für die **Identifizierung und Steuerung** von Risiken im Tagesgeschäft verantwortlich und für die **Implementierung und Durchführung von Kontrollmassnahmen** zuständig, um Risiken frühzeitig zu erkennen und zu minimieren.



Abbildung: Three-Lines-of-Defense-Modell (in Anlehnung an: Pfaff/Ruud, 2020, S. 54)

Zweite Verteidigungslinie: Diese Linie **überwacht und unterstützt die Kontrollaktivitäten der ersten Linie** und ist für die Entwicklung von Richtlinien und Verfahren, die Überwachung der Einhaltung von Vorschriften und für die Unterstützung des operativen Managements bei der Risikobewertung zuständig.

Dritte Verteidigungslinie: Die interne Revision **prüft unabhängig die Wirksamkeit der ersten und zweiten Linie**, indem sie entsprechende Audits durchführt. Im Gegensatz zu den ersten beiden Linien berichtet die dritte Linie nicht an die GL, sondern direkt an den VR bzw. wen vorhanden an das Audit Committee.

Good Governance

Gesetzliche und regulatorische Bestimmungen zu Risikomanagement und IKS

Risikobeurteilung

Gemäss OR 967 müssen Unternehmen, die von Gesetzes wegen zu einer ordentlichen Revision verpflichtet sind*, einen **Lagebericht** verfassen, im Rahmen dessen Aufschluss über die Durchführung einer **Risikobeurteilung** gegeben werden muss (OR 961c Abs. 2 Ziff. 2).

Corporate Governance Richtlinie der SIX Swiss Exchange

Die «Richtlinie betreffend Informationen zur Corporate Governance» (RLCG) gilt für alle Unternehmen, die an der Schweizer Börse SIX Swiss Exchange kotiert sind.

Existenz IKS

Gemäss OR muss die Revisionsstelle wie im Rahmen der ordentlichen Revision **prüfen, ob ein internes Kontrollsystem existiert** (OR 728a Abs. 1 Ziff. 3)*. Es ist den Unternehmen selbst überlassen, welches IKS sie für ihre Situation als angemessen erachten, **wobei die Grösse des Unternehmens, die Komplexität der Geschäftstätigkeit und das Risikoprofil für diesen Entscheid relevant sind.**

Bestimmungen regulierten Branchen und Organisationen im öffentlichen Sektor

z. B. Rundschreiben 2017/1 Corporate Governance – Banken oder Rundschreiben 2017/2 Corporate Governance – Versicherer.

z. B. Finanzhaushaltsgesetz (FHG) i. V. m. Verordnung über das Finanzhaushaltsrecht (FHV).

Swiss Code of Best Practice for Corporate Governance

Der «Swiss Code of Best Practice for Corporate Governance» (kurz «Swiss Code») wurde von economiesuisse veröffentlicht und wendet sich in Form von Leitlinien und Empfehlungen an Schweizer Gesellschaften. In Bezug auf das Risikomanagement gibt der «Swiss Code» vor, dass **der Verwaltungsrat mindestens einmal jährlich eine Risikobeurteilung vornimmt.**

Schweizer Prüfstandard PS-CH 890

Die **Aufgaben und Verantwortlichkeiten** des Verwaltungsrats, des Managements und der Revisionsstelle **in Bezug auf das IKS werden erläutert.** Weiter werden die Komponenten eines IKS beleuchtet, die folgende sind: Kontrollumfeld, Risikobeurteilungsprozess der Einheit, rechnungslegungsbezogene Informationssysteme, Kontrollaktivitäten und Überwachung der Kontrollen.

*Dazu gehören gemäss OR 727 insbesondere Publikumsgesellschaften und Unternehmen, die zwei der nachstehenden Grössen in zwei aufeinanderfolgenden Geschäftsjahren überschreiten: CHF 20 Mio. Bilanzsumme, CHF 40 Mio. Umsatz, 250 Vollzeitstellen im Jahresdurchschnitt.

02

Good Governance in der Praxis



FINANZPLATZ
Donnerstag, 17. September 2020 10:39

Wirecard-Skandal: Wer wusste alles Bescheid?

Datum: 15.11.2023

Neue Zürcher Zeitung

Medienart: Print
Medientyp: Tages- und Wochenpresse
Auflage: 80'908
Erscheinungsweise: 6x wöchentlich

Seite: 11
Fläche: 120'596 mm²

Auftrag: 3007101
Themen-Nr.: 999.222
Referenz: 90006071
Ausschnitt Seite: 1/3

Wirecard: War alles nur Scherz?
Wirecard: Wie Jan Marsalek?

Datum: 13.03.2024

Neue Zürcher Zeitung

Neue Zürcher Zeitung
8021 Zürich
044/ 258 11 11
<https://www.nzz.ch/>

Medienart: Print
Medientyp: Tages- und Wochenpresse
Auflage: 80'908
Erscheinungsweise: 6x wöchentlich

Seite: 25
Fläche: 77'443 mm²

Auftrag: 3007101
Themen-Nr.: 999.222
Referenz: 90006071
Ausschnitt Seite: 1/3

Manipulierte Kreditanträge bei der Bank Now – Credit-Suisse-Tochter schliesst temporär Filialen

Angestellte der Bank mussten ihren Arbeitsplatz räumen – Betroffene sagen, sie hätten auf Anweisung der Vorgesetzten gehandelt

Kriminelle schmieren amtliche Prüfer des Strassenverkehrsamts

Mitarbeiter sollen einem Bestechungsring angehört haben

solothurnerzeitung.ch 22.04.2024 20:53

Amtsgericht Olten

Tausende Geschädigte legte er mit falschen Rechnungen herein: Staatsanwalt fordert sechs Jahre Haft für Registerhai

Ein mutmasslicher Wirtschaftsbetrüger kassierte Hunderttausende Franken, ohne etwas dafür zu tun. Zudem engagierte er sich als «Konkursritter». Nun stand er vor dem Amtsgericht Olten-Gösgen. Ein wohl beispielloser Fall.

Auffangnetz «Fraud»

Betrugsrisiken (R)



«Soft Controls»

Unternehmenswerte / -kultur und Vorbildfunktion der Kader

z.B. Verantwortlichkeit

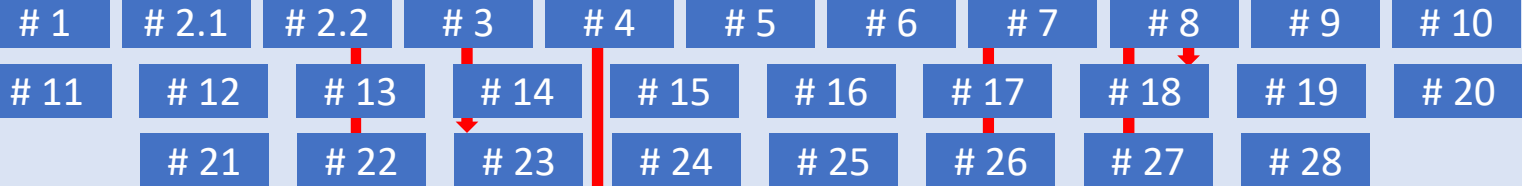
z.B. Vertrauen

z.B. Kundenfokus

«Tone from the Top», Vorbildfunktion der Kader im Vorleben der Werte

«Hard Controls»

Direkt auf Betrugsrisiken einwirkende betrugspräventive Instrumente



Indirekt auf Betrugsrisiken einwirkende, weitere betrugspräventive Instrumente

Übriges internes Kontrollsystem (Art. 728a OR)

Verhaltenskodex

Hinweisgeber-System

Sanktionen

Weisungen, Richtlinien

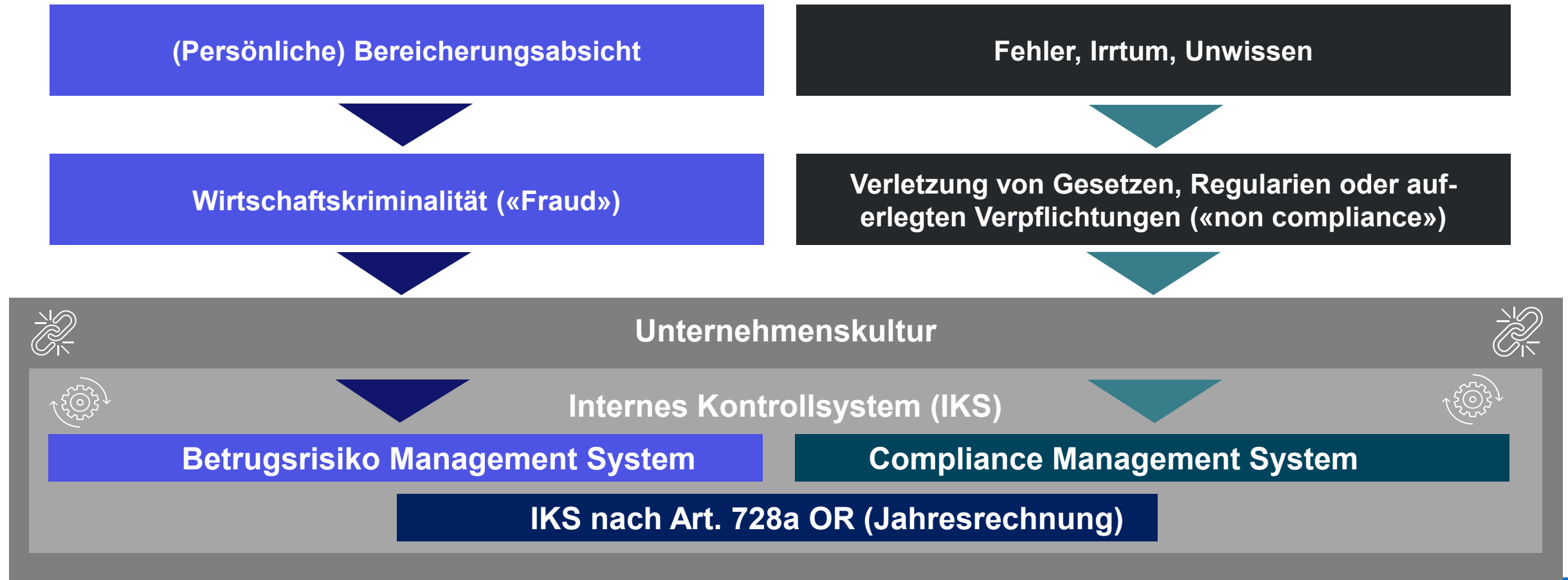
Restrisiko



Rahmenkonzept Betrugsrisiko Management

Zusammenspiel der Präventionsinstrumente

Betrugsrisiko Management vs. Compliance Management System



Fall Wirecard



Hintergrund

- Wirecard galt lange als eines der aufstrebenden Fintech-Unternehmen in Europa und wurde 2018 in den DAX-30 aufgenommen.
- Der CEO Markus Braun und der COO Jan Marsalek waren die Hauptfiguren, die den „Tone at the Top“ des Unternehmens setzten und ein Bild der Integrität und Transparenz vermittelten.
- Es stellte sich jedoch heraus, dass das Unternehmen über Jahre hinweg seine Bilanzen manipuliert hatte, um Gewinne vorzutäuschen und Investoren zu täuschen.
- Im Juni 2020 wurde bekannt, dass rund 1,9 Milliarden Euro in den Büchern fehlten, die vermutlich nie existierten.



Tone at the top

- Obwohl das Unternehmen formal über eine starke Governance-Struktur verfügte, zeigte sich in der Praxis eine Kultur der Verheimlichung und Täuschung.
- Der Vorstand war in den Betrug verwickelt, und Whistleblower-Berichte wurden systematisch ignoriert oder unterdrückt.
- Es herrschte eine toxische Kultur, in der niemand Verantwortung für Fehlverhalten übernahm.

Fall Wirecard

Red Flags (u.a. Risikomanager)

Ungewöhnlich starke Performance ohne erklärbare Gründe:

- Wirecard berichtete über Jahre hinweg aussergewöhnlich gute Zahlen, obwohl die Branche von intensiver Konkurrenz und Margendruck geprägt war.
- Ein Risikomanager hätte diese Diskrepanz genauer prüfen und nach Belegen für diese Gewinne verlangen sollen.

Komplexe Offshore-Strukturen:

- Der Grossteil der angeblichen Gewinne von Wirecard stammte von Tochtergesellschaften in Offshore-Märkten, wo die Aufsicht weniger strikt war.
- Ein Risikomanager hätte diese Offshore-Strukturen und die dort geparkten Gelder hinterfragen sollen, insbesondere, weil diese nur schwer überprüfbar waren.

Mangelnde Transparenz bei Transaktionen:

- Es gab Berichte über undurchsichtige Transaktionen, bei denen erhebliche Summen auf Konten überwiesen wurden, die schwer nachzuvollziehen waren.
- Ein Risikomanager (auch Compliance, interne/externe Prüfer) hätte tiefergehende Fragen zu diesen Transaktionen stellen und die Einhaltung der internen Richtlinien zur Transaktionsüberwachung hinterfragen sollen.
- Mangelnde Koordination innerhalb der «Assurance Funktionen»?

Whistleblower-Berichte

- Wirecard hatte mehrere Whistleblower, die auf Unregelmässigkeiten hingewiesen hatten. Die Meldungen wurden jedoch intern ignoriert oder aktiv unterdrückt.
- Ein aktiver Risikomanager hätte sicherstellen sollen, dass Whistleblower ernst genommen werden und dass Berichte systematisch untersucht werden.

Fall Wirecard

...in einer guten (perfekten) Unternehmenswelt...

Regelmässige Audits und externe Überprüfungen veranlassen:

- Interne und externe Audits könnten helfen, Unregelmässigkeiten frühzeitig zu identifizieren.
- Der Risikomanager hätte darauf bestehen können, dass solche Audits auch in schwer zugänglichen Märkten und Tochtergesellschaften durchgeführt werden.

Whistleblower ernst nehmen:

- Ein funktionierendes Whistleblower-System ist entscheidend.
- Der Risikomanager hätte sicherstellen können, dass Berichte vertraulich und ernsthaft behandelt werden und eine unabhängige Untersuchung eingeleitet wird.

Verdächtige Indikatoren überprüfen:

- Ungewöhnliche Gewinne, verdächtige Transaktionen und undurchsichtige Firmenstrukturen sind Anzeichen für potenziellen Betrug.
- Der Risikomanager (auch Compliance, interne/externe Prüfer) sollte Fragen stellen und unabhängige Analysen fordern, um zu überprüfen, ob die gemeldeten Zahlen tatsächlich plausibel sind.

Kommunikationskultur stärken:

- Der „Tone at the Top“ muss nicht nur nach aussen, sondern auch nach innen wirksam sein. Eine Kultur der Offenheit und Transparenz sollte gefördert werden, in der Bedenken frei geäußert und Missstände intern geprüft werden können.

03

Täter und Gründe für Wirtschaftskriminalität



Täter & Gründe für Wirtschaftskriminalität

Wann steigt das Betrugsrisiko in Unternehmen?

Warum fahren Sie schneller als erlaubt?

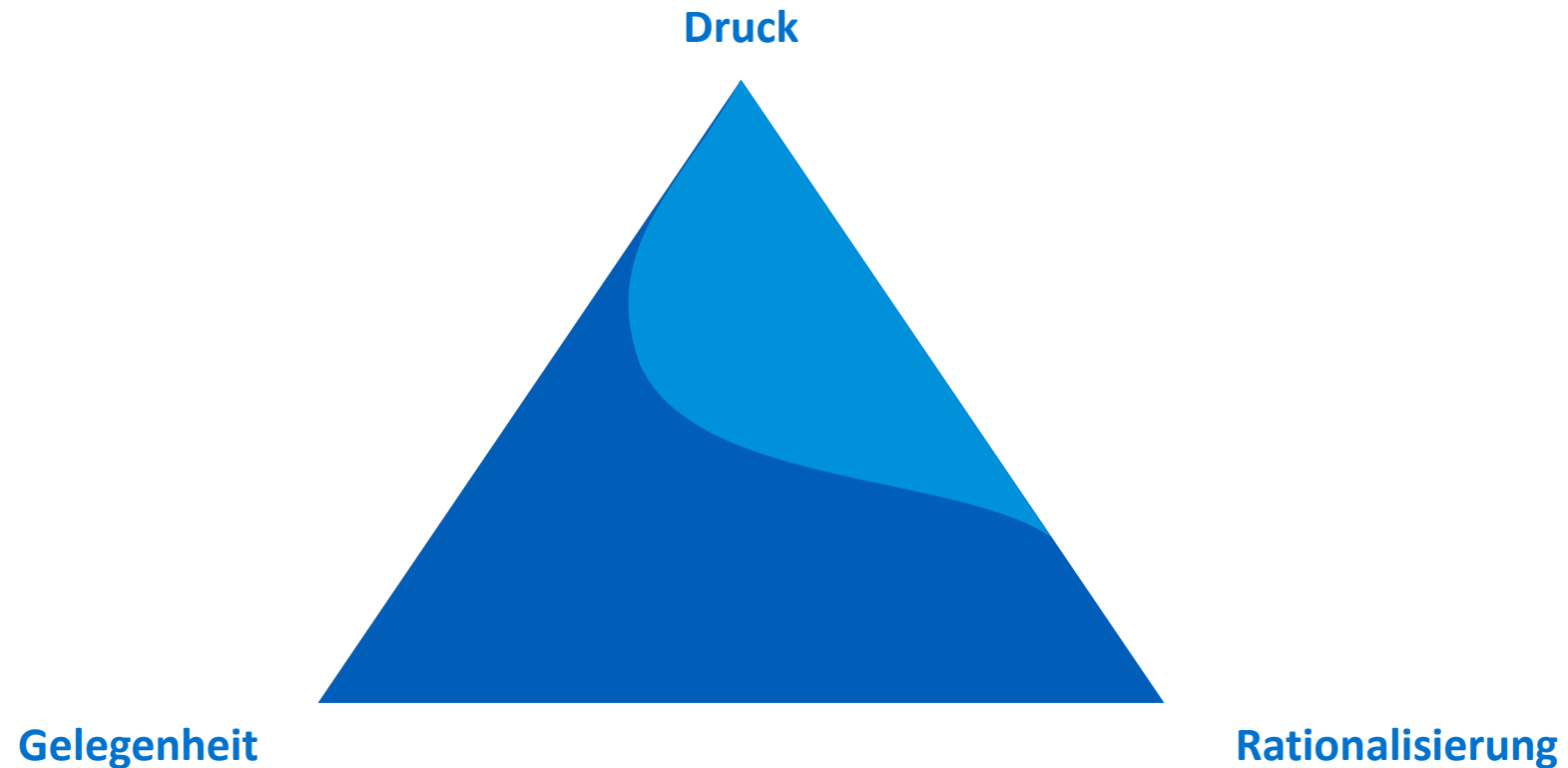


Täter & Gründe für Wirtschaftskriminalität

Wann steigt das Betrugsrisiko in Unternehmen?

Das Betrugsdreieck nach Donald R. Cressey

*(US-amerikanischer Soziologe und Kriminologe; * 27. April 1919; † 21. Juli 1987)*



Täter & Gründe für Wirtschaftskriminalität

Täterbild (1/2)



- Forschenden ist es noch nicht gelungen, einzigartige demografische Merkmale (Alter, Geschlecht, Beruf, Religion etc.) zu entdecken. Die durchschnittliche Täterschaft hat wahrscheinlich*:
 - **höheren Schulabschluss, verheiratet, keine Vorstrafen, Verhält sich sozial konform, im Alter vom jungen Erwachsenen bis ins Pensionsalter**
- Es könnte jeder von uns sein. Rund drei Viertel der Taten werden vom männlichen Geschlecht begangen, 16-mal häufiger sind es Führungskräfte als nicht leitende Angestellte.
- **Oft sind es intelligente, risikofreudige und hart arbeitende Persönlichkeiten.**
- Bei 70 % der Betrugsfälle hat der Täter mit anderen zusammengearbeitet.

*Peterson, B. K. & Zikmund P. E. (2004). 10 Truths you need to know about Fraud. Strategic Finance 2004. S. 29-34 (Fraud) und Brignola, N. (1997, August 2). Fraud Perpetrator Profile: A Short Story. National Report on Occupational Fraud and Abuse. Newsweek.

Das obenstehende Bild wurde durch ChatGPT generiert, gestützt auf die vorstehenden Merkmale / Beschreibungen.

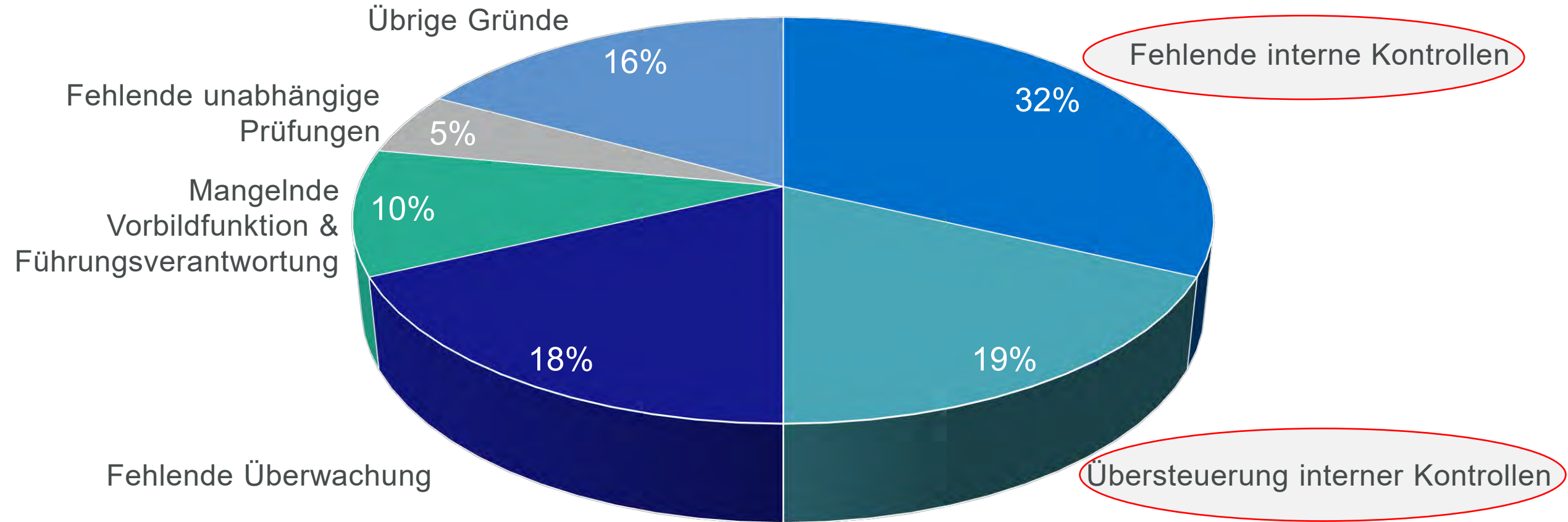
Täter & Gründe für Wirtschaftskriminalität

Täterbild (2/2)

- Wirtschaftskriminalität kommt in **43% der Fälle durch einen Hinweis** (Whistleblowing) ans Licht. 52% dieser Hinweise kommen von Mitarbeitenden (Vgl. ACFE Report 2024, Seite 24).
- Viele Fälle bleiben unentdeckt, weil Unternehmen zögern, sie öffentlich zu machen. Dadurch können Betrüger mit einem „**sauberen**“ **Arbeitszeugnis oder Strafregister** zum nächsten Arbeitgeber wechseln.
- **Eskalation von unethischem Verhalten:** es fängt klein an, schrittweise Gewöhnung (Rationalisation), zuerst kleine und harmlose Handlungen, die mit Gewissen vereinbart werden können. Anpassung des moralischen Kompasses und Abstumpfung, womit immer risikoreicheres Verhalten gezeigt wird.
- **Reaktanz bei Überregulierung:** Zu viel Kontrolle kann Mitarbeitende einschränken und bevormunden, was ihre Motivation, sich an ethische Standards zu halten, untergraben kann.

Interne Kontrollsysteme

Typische Schwächen



Quelle: «Report to the Nations – 2024 Global Study on Occupational Fraud and Abuse»; Association of Certified Fraud Examiners (ACFE), Austin, Texas, USA, 2024

Täter & Gründe für Wirtschaftskriminalität

Typische Schwächen Interner Kontrollsysteme (IKS)

Fehlende interne Kontrollen (32%)

- IKS ist oftmals nur an den gesetzlichen **Minimalanforderungen** ausgerichtet (OR 728a Abs. 1 Ziff. 3)
- Teilweise **unklar** welche Risiken das interne Kontrollsystem überhaupt abdecken soll (konkret: nur finanzielle oder auch andere Risiken?)
- Interne Prozesse sind **ständigen Veränderungen** unterworfen
- IKS = **selten das Resultat** dezidierter, fokussierter und systematischer Erhebungen von Risiken, oft «copy paste»
- Komplexe und teilweise unternehmens- resp. **länderübergreifende Prozesse** im Konzern vs. interne Kontrollsysteme pro Rechtssubjekt
- Ungenügende **Ressourcen** bspw. für die interne Revision, auch moderne Instrumente einzusetzen (bspw. künstliche Intelligenz)

Übersteuerung interner Kontrollen (19%)

- Ausnutzen von **Hierarchien** und Positionen
- **Unrealistische** Zielvorgaben und damit Zeitdruck für Mitarbeitende oft zu hoch
- Zu **viele** (vorgelagerte) interne Kontrollen
- **Kollusion** innerhalb eines Teams (bspw. Delegationen der Erstfreigaben an die persönliche Assistentin)
- **Autoritärer** Führungsstil
- IKS (und oft auch die Interne Revision) als **reine Statisten**; niemand interessiert sich wirklich für deren Erkenntnisse oder höchstens dann, wenn sie dem eigenen Macht- und Positionserhalt im Unternehmen dienen

Täter & Gründe für Wirtschaftskriminalität

Typische Schwächen von Compliance Management Systemen (CMS)

Compliance Risiken

- Mangelhafte Erhebung der **unternehmensspezifischen** Compliance Risiken (konkret: «copy paste» der Risiken von Mitbewerbern)
- Mangelhafte **Konkretisierung** der Compliance Risiken
- **Bewertung** von Compliance Risiken vs. Bewertung übriger Unternehmensrisiken
- Verantwortung zur Überwachung der Compliance Risiken oft **unklar** («1st line and 2nd line of defense»)
- Oft keine oder **mangelhafte** IKS-Kontrollen für Compliance Risiken; somit nicht Teil einer Prüfung des Design und der Effektivität der Kontrollen durch die interne und/oder externe Revision

Aufbau und Ausgestaltung

- Die Compliance Programme als Antwort auf die identifizierten Compliance Risiken sind oft nicht **spezifisch** genug (auch auf Stufe Prozess und Transaktion; bspw. aktive vs. passive Bestechung)
- **Schnittstellen** zwischen den verschiedenen unternehmensinternen «Assurance»-Funktionen sind nicht klar definiert
- Compliance Management Systeme werden **aufgesetzt** («kopiert») und widerspiegeln nicht die unternehmensspezifischen Besonderheiten (analog IKS)
- Die **Eigenwahrnehmung** betreffend Güte und Ausbaugrad des CMS aus der Sicht des Compliance Office entspricht in vielen Fällen nicht der Wahrnehmung der Mitarbeitenden
- IKS und CMS sind nicht aufeinander **abgestimmt**
- CCO steht im Glashaus und **kennt** das **Business** nur **ungenügend**

Täter & Gründe für Wirtschaftskriminalität

Typische Schwächen von Compliance Management Systemen (CMS)

Kommunikation

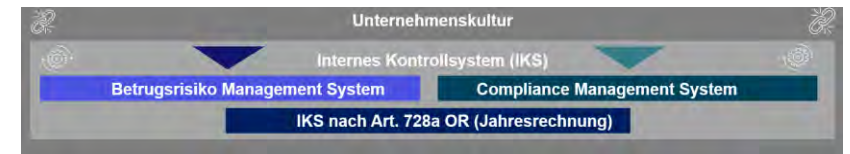
- Zu **allgemein** gehaltene Compliance Schulungen, die in der Regel nichts mit dem konkreten Arbeitsumfeld der zu schulenden Mitarbeitenden zu tun haben
- Sprache und **Ausgestaltung** interner Weisungen und Vorgaben
- Mangelhafte und uneinheitliche **Sanktionierung** von «non compliance» («*die Kleinen hängt man, die Grossen lässt man laufen*»)
- Uneinheitliche und teilweise **widersprüchliche** interne Weisungen und Reglemente

Arbeitskultur

- Compliance im weltweiten Konzern: «**one fits all**»-Lösungen versus Berücksichtigung regionaler Arbeitskulturen und –umstände
- Die tatsächlich in der Praxis von der Unternehmensleitung **vorgelebte** Unternehmenskultur hinsichtlich ethisches Verhalten entspricht nicht den Vorgaben («tone from the top»)

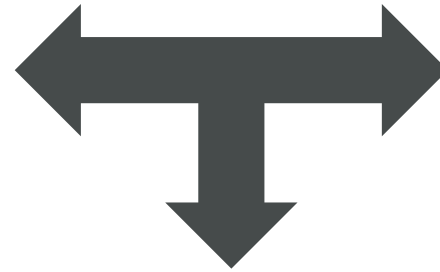
Täter & Gründe für Wirtschaftskriminalität

Begünstigende Faktoren



Faktoren, die Fehlverhalten im Unternehmen begünstigen

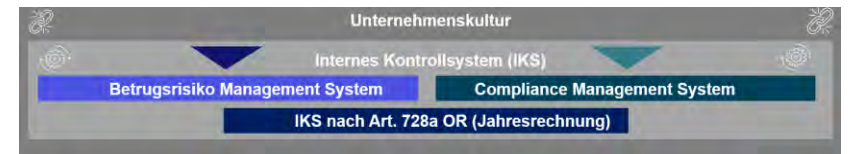
**Mangelhaftes Internes
Kontrollsystem (IKS)**



**Mangelhaftes Compliance
Management System (CMS)**

Schwächen in der Unternehmenskultur

Täter & Gründe für Wirtschaftskriminalität «Tone from the Top»



«Grundzüge des Compliance Management Systems von Wirecard»

III. Compliance Programm

1. Tone from the Top

Der Vorstand toleriert kein rechtswidriges oder unethisches Verhalten und verzichtet auf Geschäftsvorgänge, die gegen Compliance-Grundsätze verstoßen. Der Vorstand ist zur Einhaltung gesetzlicher Vorschriften verpflichtet und erwartet von seinen Mitarbeitern, dass diese verantwortungsbewusst und gesetzeskonform handeln. Zu den in unserem Code of Conduct niedergelegten Werten bekennt sich der Vorstand ausdrücklich. Fehlverhalten wird im Einzelfall entsprechend sanktioniert.

04

Prävention: Unternehmenskultur



Prävention: Unternehmenskultur

Praxisbeispiel

Angestellte einer Bankfiliale, in welcher Kundengelder veruntreut wurden



«Es ist mir schon aufgefallen und ich habe mich auch gefragt, was für Bargeldtransaktionen XYZ jeweils ausführte.

Aufgrund der internen Weisung, wonach wir mit Entlassung rechnen müssen, wenn wir Einsicht in Bankkonten unserer Arbeitskollegen nehmen, habe ich lieber nichts gesagt. Auch wenn wir gemäss der Weisung «Hinweisgeber» aufgefordert sind, mögliches Fehlverhalten zu melden. Ich wusste nicht, was passiert, wenn ich etwas melde. Das HR ist in einer anderen Stadt.

Weiter ging ich davon aus, dass dem Vorgesetzten von XYZ diese Transaktionen sicherlich auch aufgefallen sind.»

Einleitung

«Why good people sometimes do bad things»

Elemente, die einen wesentlichen Einfluss auf die ethische Kultur eines Unternehmens haben.



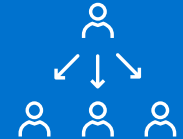
Klarheit der Standards



Identifikation



Transparenz



Vorbildfunktion



Realisierbarkeit



Durchsetzung



Offenheit

Quelle: Modell nach Kaptein, Muel: «The Living Code - Embedding Ethics into the Corporate DNA», 2008, S. 82 - 87

Prävention: Unternehmenskultur

Klarheit der Standards

Kurzbeschreibung

- Es ist den Mitarbeitenden auf allen Stufen klar und gut verständlich, welche Verhaltensweisen von ihnen erwartet werden
- Verstehen die Mitarbeitenden auf allen Stufen, warum diese Werte und Verhaltensnormen existieren und wie sie persönlich dazu beitragen können, diesen nachzukommen resp. diese zu leben?

Illustratives Beispiel

- Eine Bankangestellte meldete ein von ihr beobachtetes Fehlverhalten ihres Arbeitskollegen deswegen nicht, weil zwei interne Weisungen widersprechende Vorgaben enthielten, und sie für sich selbst entschied, welche dieser beiden Weisungen sie als bedeutender einschätzte

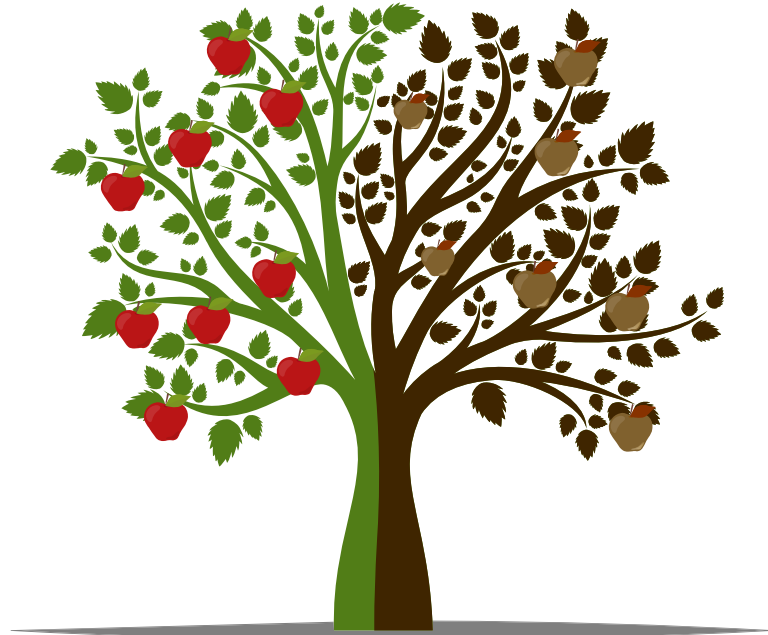
Instrumente

- Konsistente Kommunikation ausgehend von der obersten Geschäftsleitung («Tone from the Top»)
- Unternehmensspezifischer Verhaltenskodex
- Spezifische Schulungen und Sensibilisierungsmassnahmen
- «House of policies»
- Klar definierte Schnittstellen zwischen den «Assurance»-Funktionen
- Sprache und Verständlichkeit der Standards

Prävention: Unternehmenskultur

Vorbildfunktion

Kurzbeschreibung



Illustratives Beispiel

- Eine bei einem Unternehmen in der Schweiz durchgeführte jährliche Mitarbeiterbefragung zeigte einen starken Rückgang der Zustimmungsrate betreffend Vertrauen der Belegschaft in den Verwaltungsrat, nachdem in der Presse negative und kritische Berichterstattungen über einen Verwaltungsrat erschienen sind

Instrumente

- «Walk the Talk»
- «360° Feedback Reviews»
- Sanktionierung von Vorgesetzten, die die Werte des Unternehmens nicht leben
- Zielvereinbarungen
- Selektion von Führungskräften (Einstellung, Beförderung)
- Förderung der unternehmensinternen «Verstärker», die gemeinhin als gute Vorbilder wahrgenommen werden

Prävention: Unternehmenskultur

Identifikation

Kurzbeschreibung

- Eine hohe Identifikation der Mitarbeitenden mit dem Unternehmen führt dazu, dass die Mitarbeitenden motiviert und bereit sind, die Werte des Unternehmens zu verteidigen und aufrecht zu halten
- Stehen die Mitarbeitenden hinter den Werten und Zielen des Unternehmens?

Illustratives Beispiel



Instrumente

- Einschwören auf ein gemeinsames Ziel
- Begeisterung für den eigenen Arbeitgeber fördern, so dass Mitarbeitende stolz auf ihren Arbeitgeber sind

Prävention: Unternehmenskultur

Realisierbarkeit

Kurzbeschreibung

- Können die Mitarbeitenden, mit denen ihnen zur Verfügung stehenden Ressourcen und Kompetenzen, die ihnen gesteckten Ziele überhaupt erreichen?
- Oder sind sie quasi gezwungen, Werte zu vernachlässigen und Verhaltensnormen zu brechen, um die Ziele erreichen zu können?

Illustratives Beispiel

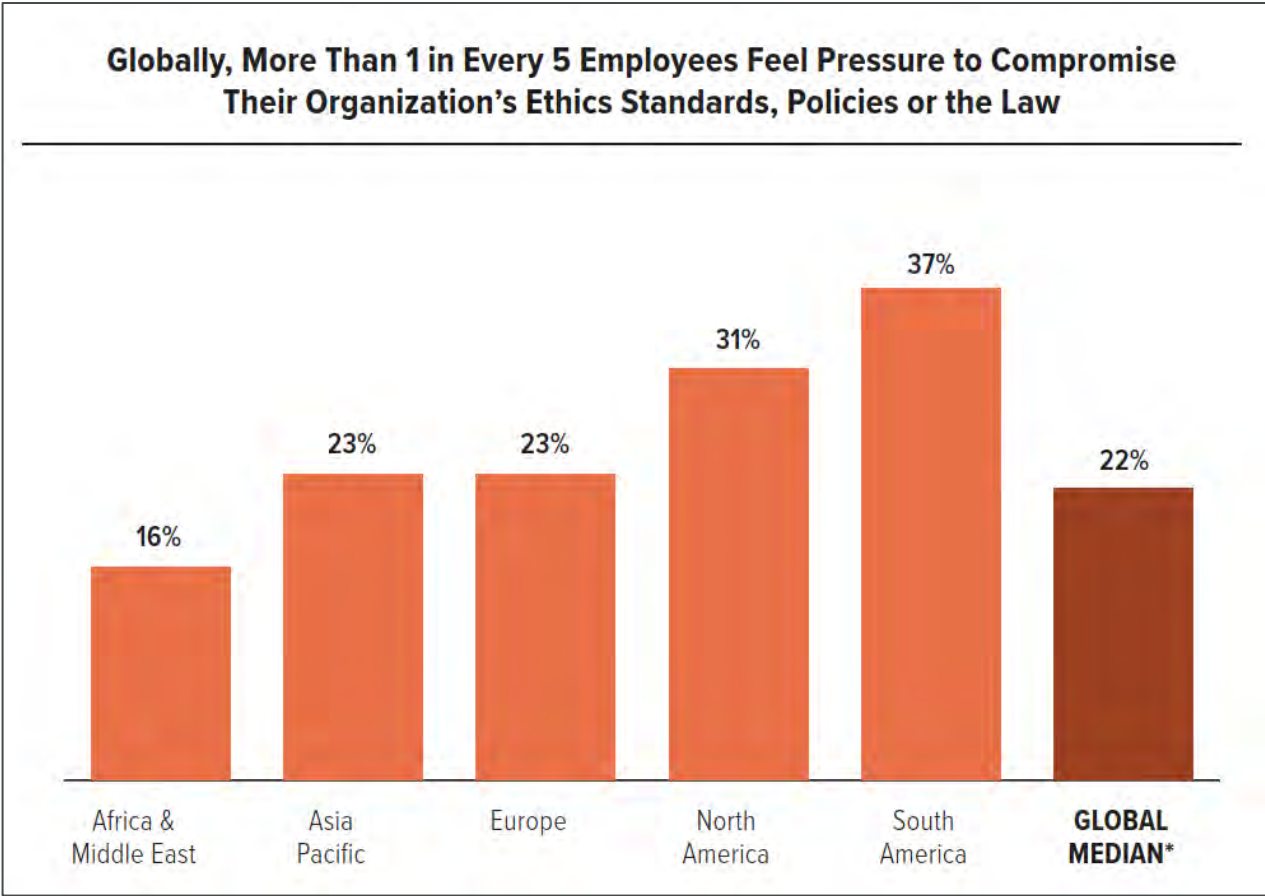
- Gemäss einer Umfrage von ECI - Ethics & Compliance Initiative (USA) - fühlt sich weltweit jeder fünfte Mitarbeitende unter Druck, interne Regeln und gesetzliche Vorgaben zu umgehen, um die Ziele erreichen zu können.

Instrumente

- Ausreichende Ressourcen zur Erledigung der Aufgaben
- Realistische Zielvorgaben
- Aufgabenzuweisungen

Prävention: Unternehmenskultur

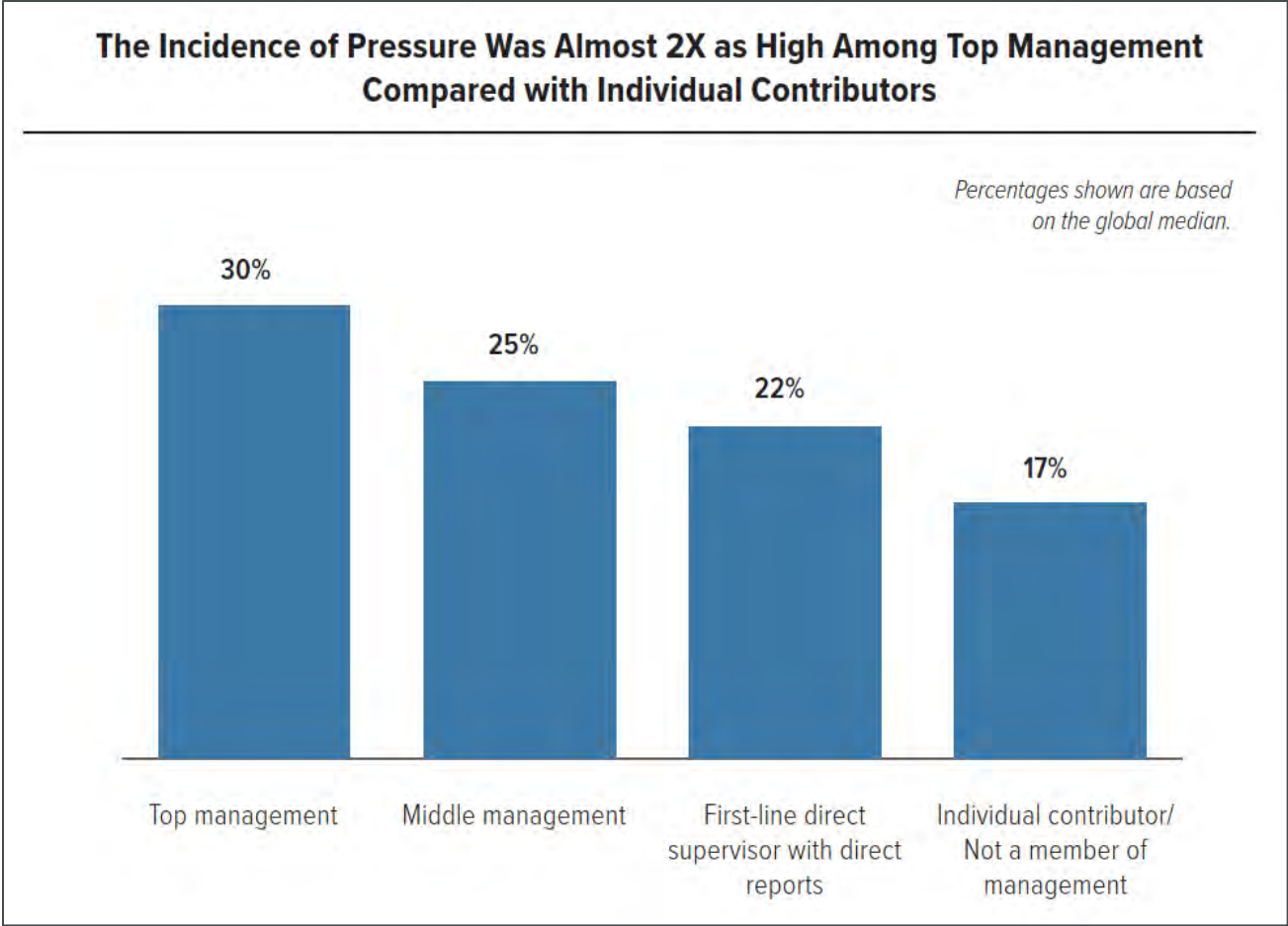
Realisierbarkeit



Quelle: «2020 Global Business Ethics Survey», ECI - Ethics & Compliance Initiative (siehe auch: www.ethics.org)

Prävention: Unternehmenskultur

Realisierbarkeit



Quelle: «2020 Global Business Ethics Survey», ECI - Ethics & Compliance Initiative (siehe auch: www.ethics.org)

Prävention: Unternehmenskultur

Transparenz

Kurzbeschreibung

- Eine hohe unternehmensinterne Transparenz stellt sicher, dass
 - (internes) Fehlverhalten besser erkannt wird
 - was wiederum dazu führt, dass ein Unternehmen schneller auf Fehlverhalten reagieren kann
- Schon nur die Aussicht darauf, dass eigenes Fehlverhalten aufgedeckt wird, hat eine präventive Wirkung

Illustratives Beispiel

- Sprayereien in dunklen vs. belebten und hell ausgeleuchteten Passagen

Instrumente

- Kommunikation von Fehlverhalten in der Organisation

Prävention: Unternehmenskultur

Offenheit

Kurzbeschreibung

- Wie offen fühlen sich Mitarbeitende, Dilemmas offen anzusprechen? Ohne Angst vor Repressalien?

Illustratives Beispiel

- Als leitender Angestellter der Abteilung «Events» organisiere ich regelmässig grössere Anlässe, zu welchen wir unsere Kunden in repräsentative Hotels in der ganzen Schweiz einladen

Eines Tages offeriert mir der Direktor eines Hotels ein Gratiswochenende mit meiner ganzen Familie im neu renovierten Hotel

Instrumente

- Dilemma-Situationen offen ansprechen (bspw. Besprechungen im Team)
- Dilemma-Situationen intern kommunizieren (bspw. Intranet oder in Schulungen)
- Dilemma-Situationen als illustrative Beispiele in den Verhaltenskodex des Unternehmens aufnehmen

Prävention: Unternehmenskultur

Durchsetzung

Kurzbeschreibung

- Fehlverhalten eines Vorgesetzten oder eines Mitarbeitenden muss sanktioniert werden
- Keine Sanktionen auszusprechen bedeutet, dass bspw. ein Verhaltenskodex nicht für alle Mitarbeitenden die gleiche Verbindlichkeit hat

Illustratives Beispiel

- Wiederholtes und konsequentes Umgehen von internen Regeln und Weisungen ohne Konsequenzen resp. Sanktionen führt dazu, dass die Weisungen des Unternehmens nicht mehr ernst genommen und nicht mehr eingehalten werden

Instrumente

- Einheitliche Sanktionierungspraxis
- Verantwortlichkeiten für Sanktionierungen festlegen (Linie vs. zentrale Stelle)
- ggf. Schaffen eines Gremiums (bspw. «Ethics Committee»)

Prävention: Unternehmenskultur

Praxisbeispiel (Lösung)



«Es ist mir schon aufgefallen und ich habe mich auch gefragt, was für Bargeldtransaktionen XYZ jeweils ausführte.»

→ **fehlende oder nicht wirksame interne Kontrollen (mangelhaftes IKS)**

Aufgrund der internen Weisung, wonach wir mit Entlassung rechnen müssen, wenn wir Einsicht in Bankkonten unserer Arbeitskollegen nehmen, habe ich lieber nichts gesagt. Auch wenn ich eine Weisung «Hinweisgeber» aufgefordert wurde, mögliches Fehlverhalten zu melden. Ich wusste nicht, was passiert, wenn ich etwas melde. Das HR ist in einer anderen Stadt.

Klarheit

→ **widersprüchliche interne Compliance Weisungen (mangelhaftes CMS)**

Offenheit

Weiter ging ich davon aus, dass dem Vorgesetzten von XYZ diese Transaktionen sicher auch aufgefallen sind.»

→ **Angst vor Vergeltung und fehlendes Vertrauen (Unternehmenskultur)**

05

Werkzeuge

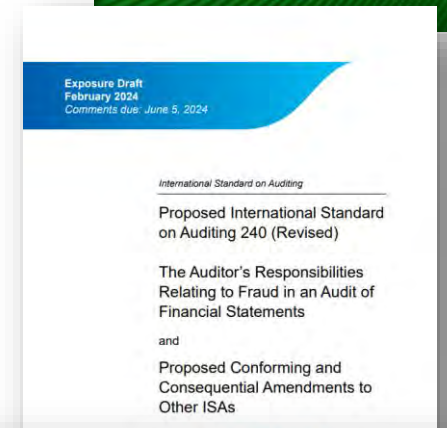
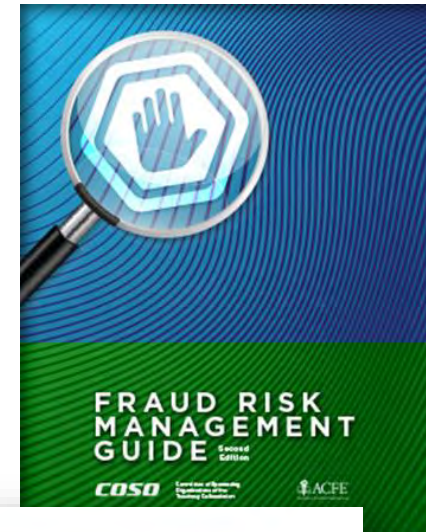


Betrugsprävention

Internationale regulatorische Entwicklungen «Fraud Risk Management»

- ❑ COSO** « Fraud Risk Management Framework » (seit 2016; updated in 2023)
 - ❑ Erster “Fraud Risk Management Guide” in 2016, mit einem wichtigen Update in 2023
 - ❑ 5 Bereiche: 1-Control environment (“Tone at the Top”, Leadership, Support), 2-Fraud risk analysis, 3-Control activities (via prevention and detection), 4-Information & Communication and 5-Monitoring.
- ❑ International Standard on Auditing (ISA) 240 (bestehender Standard, Revision 2024)
 - ❑ Draft, Feb. 2024 – Revision: “*Renforcing the professional skepticism throughout the audit*”
 - ❑ “*Applying a fraud lens on risk identification and assessment*”
- ❑ ISO-Standard 37003 (Entwurf) – Coming soon
 - ❑ Draft, Mai 2024: Guidance für “Fraud Control Management Systems”

** “Committee of Sponsoring Organizations of the Treadway Commission” is a reputed US-based global organization. It aims at “developing thought leadership that enhances internal control, risk management (ERM), governance and fraud deterrence”.



06

Interne Untersuchung



Best Practice-Ansätze

Ausgewählte Aspekte einer internen Untersuchung

"Anzeichen für Fehlverhalten" -
Vertrauen Sie Ihrem Bauchgefühl.

Gelöschte E-Mails" -
Setzen Sie das so genannte "Journaling" ein.

"Führen von Interviews" -
Die meisten Antworten kennen.

"Sanktionen sind notwendig" -
Führen Sie eine "Sanktionspolitik" ein.



"Grenzüberschreitende Ermittlungen" - Lassen Sie sich beraten, es ist ein Minenfeld.

"Riesige Datenmengen" - Arbeit mit Hypothesen.

"Einen Bericht zu schreiben ist eine Kunst" - Keine Meinungen, nur Fakten.

"Niemand ist perfekt" - Führen Sie eine Ursachenanalyse durch.

Interne Untersuchungen

Einige Tipps aus der Praxis, was Sie beim Eingang einer Meldung unbedingt tun sollten

✓	Ruhe bewahren	✓	Beweise sichern
✓	Policy	✓	Arbeitsrechtliche Massnahmen
✓	Externe Kommunikation	✓	Business Continuity (BCM)

Interne Untersuchungen

Einige Tipps aus der Praxis, was Sie beim Eingang einer Meldung **NICHT** tun sollten!

X	Vorurteile	X	Direkte Konfrontation
X	Trivialisierung	X	Self made eDiscovery
X	Falscher Fokus	X	Unüberlegte Information und Kommunikation

07

Key Take aways / Food for thought



Key Take aways / Food for thought

- «Man hat es immer kommen sehen»
- AKV / Schnittstellen zwischen «three lines of defense» definieren
- Betrugsaspekte / Fraud beachten (Risk vs. Compliance vs. Betrugsrisiken)
- Verbündete suchen innerhalb Assurance Funktionen
- Unternehmensspezifische Betrugsrisiken ermitteln (z.B. Workshops); auch auf Stufe VR/GL
- Mitarbeitende schulen / sensibilisieren, «in die Welt des Fraud führen»
- Problematik «zu viele Kontrollen», weniger ist mehr
- «Täter» wissen, dass Fragen kommen
- Thema «Fraud» für GL/VR spannend?



Quelle: <https://g-wie-gastro.de/mehr/ideen-und-tipps/tipps-der-woche-archiv/52-der-fisch-faengt-am-kopf-an-zu-stinken.html>

Kontakt

Forvis Mazars

Daniel Spicher, Executive Director

Daniel.Spicher@mazars.ch

Forvis Mazars Group SC ist ein unabhängiges Mitglied von Forvis Mazars Global, einem führenden Professional Services-Netzwerk. Als international integrierte Partnerschaft ist die Forvis Mazars Group in über 100 Ländern und Regionen der Welt tätig und auf die Bereiche Audit, Tax sowie Advisory spezialisiert. Die Partnerschaft greift auf die Expertise und das kulturelle Know-how von mehr als 35.000 Mitarbeitenden weltweit zurück, um Kundinnen und Kunden jeder Grösse in jeder Phase ihrer Entwicklung zu unterstützen. In der Schweiz arbeiten mehr als 400 Expertinnen und Experten an zehn verschiedenen Standorten.

© Forvis Mazars 2024. All rights reserved.

Folgen Sie uns

LinkedIn:

<https://www.linkedin.com/company/forvis-mazars-in-switzerland>

Facebook:

<https://www.facebook.com/forvismazarsinswitzerland>

Instagram:

<https://www.instagram.com/forvismazarsinswitzerland>

Mehr Informationen unter www.forvismazars.com/ch