

DIN ISO 37002



ICS 03.100.01; 03.100.02; 03.100.70

**Hinweismanagementsysteme –
Leitlinien (ISO 37002:2021)**

Whistleblowing management systems –
Guidelines (ISO 37002:2021)

Systèmes de management des alertes –
Lignes directrices (ISO 37002:2021)

Gesamtumfang 46 Seiten

DIN-Normenausschuss Organisationsprozesse (NAOrg)

Inhalt

	Seite
Nationales Vorwort	4
Nationaler Anhang NA (informativ) Literaturhinweise	5
Vorwort	6
Einleitung	7
1 Anwendungsbereich	10
2 Normative Verweisungen	10
3 Begriffe	10
4 Kontext der Organisation	17
4.1 Verstehen der Organisation und ihres Kontextes	17
4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien	18
4.3 Festlegen des Anwendungsbereichs des Hinweismanagementsystems	18
4.4 Hinweismanagementsystem	19
5 Führung	19
5.1 Führung und Verpflichtung	19
5.1.1 Oberstes Organ	19
5.1.2 Oberste Leitung	20
5.2 Politik zum Hinweisgeben	21
5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation	22
5.3.1 Oberste Leitung und oberstes Organ	22
5.3.2 Hinweismanagementfunktion	22
5.3.3 Delegierte Entscheidungsfindung	23
6 Planung	23
6.1 Maßnahmen zum Umgang mit Risiken und Möglichkeiten	23
6.2 Ziele des Hinweismanagementsystems und Planung zu deren Erreichung	24
6.3 Planung von Änderungen	25
7 Unterstützung	25
7.1 Ressourcen	25
7.2 Kompetenz	25
7.3 Sensibilisierung	26
7.3.1 Allgemeines	26
7.3.2 Personalschulung und Sensibilisierungsmaßnahmen	26
7.3.3 Schulung für Führungskräfte und andere spezifische Funktionen	27
7.4 Kommunikation	28
7.5 Dokumentierte Information	29
7.5.1 Allgemeines	29
7.5.2 Erstellen und Aktualisieren dokumentierter Information	29
7.5.3 Lenkung dokumentierter Information	29
7.5.4 Datenschutz	30
7.5.5 Vertraulichkeit	30
8 Betrieb	31
8.1 Betriebliche Planung und Steuerung	31
8.2 Entgegennahme von Meldungen über Fehlverhalten	33
8.3 Bewertung von Meldungen über Fehlverhalten	35
8.3.1 Bewertung des gemeldeten Fehlverhaltens	35
8.3.2 Bewertung und Vorbeugung von Risiken nachteiliger Behandlung	36
8.4 Behandeln von Meldungen über Fehlverhalten	37
8.4.1 Behandeln von gemeldetem Fehlverhalten	37
8.4.2 Schutz und Unterstützung des Hinweisgebers	38
8.4.3 Behandeln von nachteiliger Behandlung	38
8.4.4 Schutz der Person(en), die Gegenstand einer Meldung ist/sind	39
8.4.5 Schutz von relevanten interessierten Parteien	39

8.5	Abschluss von Fällen von Hinweisgeben	40
9	Bewertung der Leistung	41
9.1	Überwachung, Messung, Analyse und Bewertung	41
9.1.1	Allgemeines	41
9.1.2	Bewertungsindikatoren	41
9.1.3	Informationsquellen	42
9.2	Internes Audit	42
9.2.1	Allgemeines	42
9.2.2	Programm des internen Audits	43
9.3	Managementbewertung	43
9.3.1	Allgemeines	43
9.3.2	Eingaben für die Managementbewertung	43
9.3.3	Managementbewertungsergebnisse	44
10	Verbesserung	44
10.1	Fortlaufende Verbesserung	44
10.2	Nichtkonformität und Korrekturmaßnahmen	44
	Literaturhinweise	46

Bilder

Bild 1 — Übersicht eines Hinweismanagementsystems	9
Bild 2 — Beziehung zwischen dem Hinweismanagementsystem und anderen Organisationsprozessen und -systemen	18
Bild 3 — Verfahrensschritte des Hinweismanagementsystems	33

Nationales Vorwort

Dieses Dokument enthält die deutsche Übersetzung der Internationalen Norm ISO 37002:2021, die vom Technischen Komitee ISO/TC 309 „Governance of organizations“ erarbeitet wurde, dessen Sekretariat von BSI (Verinigtes Königreich) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 175-00-01 AA „Governance und Compliance-Management“ im DIN-Normenausschuss Organisationsprozesse (NAOrg).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. DIN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO/IEC 27001	siehe	DIN EN ISO/IEC 27001
ISO/IEC 27018	siehe	DIN EN ISO/IEC 27018
ISO 31000	siehe	DIN ISO 31000
ISO 37001:2016	siehe	DIN ISO 37001:2018-05
ISO 37301	siehe	DIN ISO 37301

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 27001, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen*

DIN EN ISO/IEC 27018, *Informationstechnik — Sicherheitsverfahren — Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung*

DIN ISO 31000, *Risikomanagement — Leitlinien*

DIN ISO 37001:2018-05, *Managementsysteme zur Korruptionsbekämpfung — Anforderungen mit Leitlinien zur Anwendung (ISO 37001:2016)*

DIN ISO 37301, *Compliance-Managementsysteme — Anforderungen mit Leitlinien zur Anwendung*

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsinstitute (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird üblicherweise von Technischen Komitees von ISO durchgeführt. Jede Mitgliedsorganisation, die Interesse an einem Thema hat, für welches ein Technisches Komitee gegründet wurde, hat das Recht, in diesem Komitee vertreten zu sein. Internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO stehen, nehmen ebenfalls an der Arbeit teil. ISO arbeitet bei allen elektrotechnischen Normungsthemen eng mit der Internationalen Elektrotechnischen Kommission (IEC) zusammen.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Es sollten insbesondere die unterschiedlichen Annahmekriterien für die verschiedenen ISO-Dokumentenarten beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/TC 309, *Governance of organizations* erarbeitet.

Feedback oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html zu finden.

Einleitung

Unter Hinweisgeben wird die Meldung von Hinweisen über vermutetes Fehlverhalten oder das Risiko von Fehlverhalten verstanden. Studien und die Erfahrung zeigen, dass viele Fälle von Fehlverhalten den betroffenen Organisationen durch Meldungen von Personen bekannt werden, die innerhalb der Organisation tätig sind oder eng mit dieser zusammenarbeiten.

Organisationen erwägen zunehmend, als Reaktion auf behördliche Vorgaben oder auf freiwilliger Basis interne Richtlinien und Prozesse für Hinweisgeben einzuführen oder zu verbessern.

Dieses Dokument bietet Organisationen Leitlinien für die Festlegung, Umsetzung, Pflege und Verbesserung eines Hinweismanagementsystems, um die folgenden Ergebnisse zu erzielen:

- a) die Meldung von Fehlverhalten zu fördern und zu unterstützen;
- b) Unterstützung und Schutz von Hinweisgebern und anderen betroffenen interessierten Parteien;
- c) sicherzustellen, dass Meldungen über Fehlverhalten ordnungsgemäß und zeitnah nachgegangen wird;
- d) Verbesserung der Organisationskultur und -führung;
- e) Verringerung der Risiken von Fehlverhalten.

Zu den potenziellen Vorteilen für die Organisation gehören:

- Möglichkeit für die Organisation, Fehlverhalten frühestmöglich zu erkennen und zu behandeln;
- zur Verhinderung oder Minimierung des Verlusts von Vermögenswerten und zur Wiedererlangung verlorener Vermögenswerte beizutragen;
- die Einhaltung der Richtlinien und Verfahren der Organisation sowie der gesetzlichen und sozialen Verpflichtungen sicherzustellen;
- Personal zu gewinnen und zu halten, das sich den Werten der Organisation und der Organisationskultur verpflichtet fühlt;
- der Gesellschaft, den Märkten, den Aufsichtsbehörden, den Eigentümern und anderen interessierten Parteien die Einhaltung fundierter ethischer Governance-Aktivitäten zu demonstrieren.

Ein wirksames Hinweismanagementsystem schafft Vertrauen in die Organisation, indem:

- die Führung ihre Entschlossenheit zeigt, Fehlverhalten zu verhindern und zu behandeln;
- Mitarbeiter motiviert werden, Fehlverhalten frühzeitig zu melden;
- vermieden und verhindert wird, dass Hinweisgeber und andere Beteiligte aufgrund ihres Handelns Nachteile erleiden;
- eine Kultur der Offenheit, Transparenz, Integrität und Verantwortlichkeit zu fördern.

Dieses Dokument gibt Organisationen Leitlinien für die Schaffung eines Hinweismanagementsystems auf Basis der Grundsätze von Vertrauen, Unparteilichkeit und Schutz. Es kann je nach Größe, Beschaffenheit und Komplexität der Aktivitäten der Organisation sowie der Rechtsordnung, innerhalb der sie tätig ist, angepasst werden und unterschiedlich angewendet werden. Es kann eine Organisation dabei unterstützen, ihre bestehenden Richtlinien und Verfahren für Hinweisgeben zu verbessern oder die Einhaltung der geltenden Gesetzgebung zu Hinweisgeben zu sichern.

Dieses Dokument wendet die „harmonisierte Struktur“ (en: harmonized structure) an (d. h. feste Abschnittsreihenfolge, einheitlicher Text und einheitliche Terminologie), die von der ISO erarbeitet wurde, um die Internationalen Normen für Managementsysteme anzugleichen. Organisationen können dieses Dokument als eigenständige Leitlinie oder neben anderen Managementsystem-Normen in ihrer Organisation anwenden, unter anderem um auf Hinweisgeben betreffende Anforderungen in anderen ISO-Managementsystemen einzugehen.

Bild 1 bietet eine konzeptionelle Übersicht eines empfohlenen Hinweismanagementsystems und zeigt, wie die Prinzipien „Vertrauen“, „Unparteilichkeit“ und „Schutz“ sämtliche Elemente eines derartigen Systems überlagern.

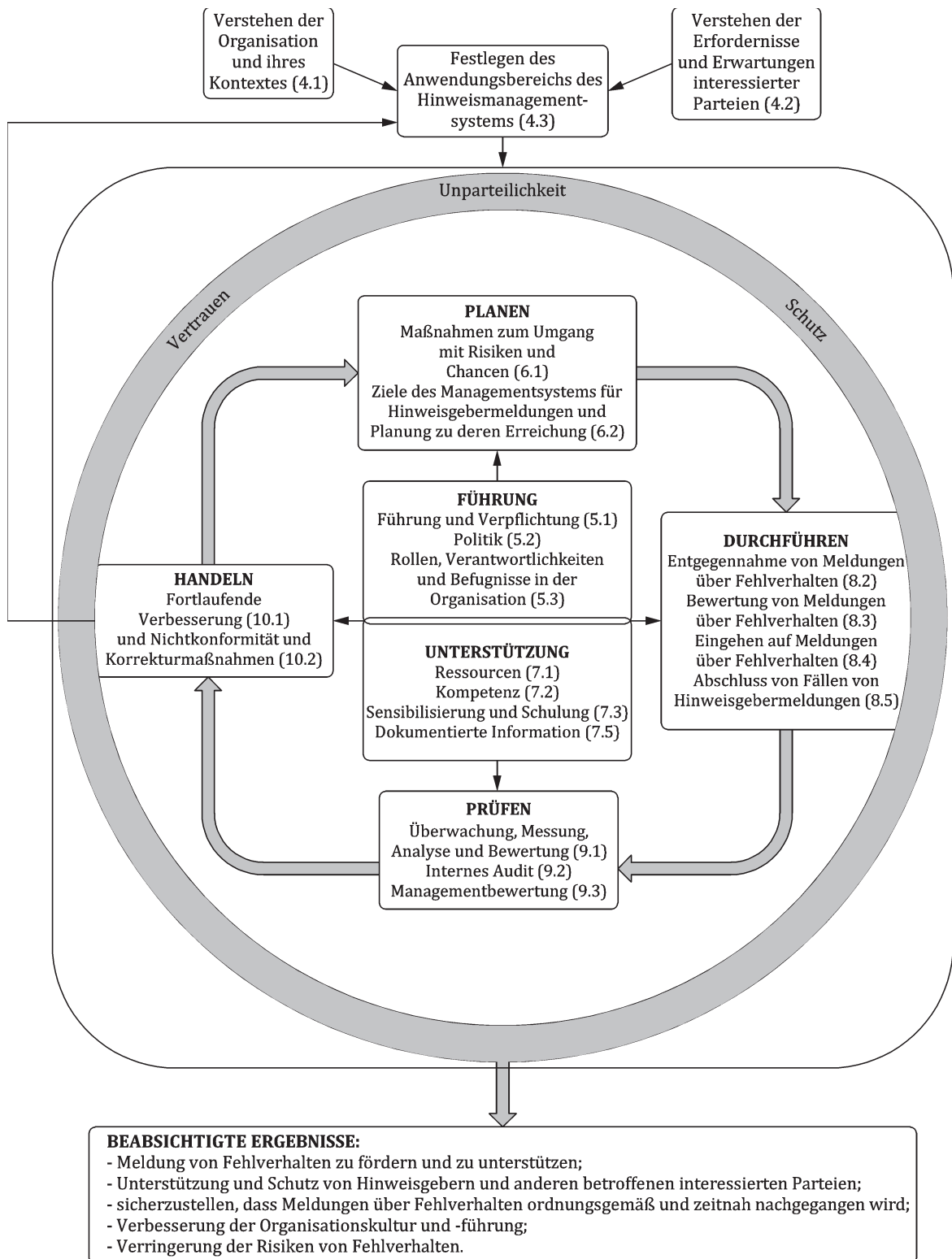


Bild 1 — Übersicht eines Hinweismanagementsystems

1 Anwendungsbereich

Dieses Dokument enthält Leitlinien für die Festlegung, Umsetzung und Aufrechterhaltung eines wirksamen Hinweismanagementsystems auf Basis der Grundsätze Vertrauen, Unparteilichkeit und Schutz mit den folgenden vier Schritten:

- a) Entgegennahme von Meldungen über Fehlverhalten;
- b) Bewertung von Meldungen über Fehlverhalten;
- c) Behandeln von Meldungen über Fehlverhalten;
- d) Abschluss von Fällen von Hinweisgeben.

Die Leitlinien dieses Dokuments sind allgemein gefasst und dafür vorgesehen, für alle Organisationen anwendbar zu sein, unabhängig vom Typ, der Größe und Art der Tätigkeit und ob es sich um öffentliche, privatwirtschaftliche oder gemeinnützige Sektoren handelt.

Der Umfang der Anwendung dieser Leitlinien hängt von den in 4.1, 4.2 und 4.3 festgelegten Faktoren ab. Das Hinweismanagementsystem kann eigenständig oder in ein übergeordnetes Managementsystem integriert sein.

2 Normative Verweisungen

Es gibt keine normativen Verweisungen in diesem Dokument.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp/ui>
- IEC Electropedia: verfügbar unter <https://www.electropedia.org>

3.1

Managementsystem

Satz zusammenhängender und sich gegenseitig beeinflussender Elemente einer *Organisation* (3.2), um *Politiken* (3.7), *Ziele* (3.25) und *Prozesse* (3.27) zum Erreichen dieser Ziele festzulegen

Anmerkung 1 zum Begriff: Ein Managementsystem kann eine oder mehrere Disziplinen behandeln.

Anmerkung 2 zum Begriff: Die Elemente des Managementsystems beinhalten die Struktur der Organisation, Rollen und Verantwortlichkeiten, Planung sowie Betrieb.

Anmerkung 3 zum Begriff: Dies ist eine(r) der gemeinsamen Begriffe und Kerndefinitionen der harmonisierten Struktur für ISO-Managementsystemnormen.

3.2

Organisation

Person oder Personengruppe, die eigene Funktionen mit Verantwortlichkeiten, Befugnissen und Beziehungen hat, um ihre *Ziele* (3.25) zu erreichen

Anmerkung 1 zum Begriff: Der Begriff Organisation umfasst unter anderem Einzelunternehmer, Gesellschaft, Konzern, Firma, Unternehmen, Behörde, Handelsgesellschaft, Wohltätigkeitsorganisation, Institution, oder Teile oder eine Kombination der genannten, ob eingetragen oder nicht, öffentlich oder privat.

Anmerkung 2 zum Begriff: Wenn die Organisation Teil einer größeren Einheit ist, bezieht sich der Begriff „Organisation“ nur auf den Teil der größeren Einheit, der in den Anwendungsbereich des *Managementsystems* (3.1) für *Hinweisgeben* (3.10) fällt.

Anmerkung 3 zum Begriff: Dies ist eine(r) der gemeinsamen Begriffe und Kerndefinitionen der harmonisierten Struktur für ISO-Managementsystemnormen.

3.3

Personal

Mitglieder des obersten Organs und der obersten Leitung, leitende Angestellte, Beschäftigte, Zeitpersonal oder Leiharbeiter und Freiwillige *der Organisation* (3.2)

[QUELLE: ISO 37001:2016, 3.25, modifiziert — Anmerkungen 1 und 2 zum Begriff wurden gestrichen.]

3.4

interessierte Partei

Person oder *Organisation* (3.2), die eine Entscheidung oder Tätigkeit beeinflussen kann, die davon beeinflusst sein kann oder sich davon beeinflusst fühlen kann

Anmerkung 1 zum Begriff: Eine interessierte Partei kann der Organisation angehören oder außerhalb der Organisation sein.

Anmerkung 2 zum Begriff: Zu den interessierten Parteien können unter anderem Personen gehören, die melden, Personen, die Gegenstand dieser Meldungen sind, Zeugen, *Personal* (3.3), Arbeitnehmervertreter, Lieferanten, Dritte, die Öffentlichkeit, Medien, Aufsichtsbehörden und die Organisation als Ganzes.

Anmerkung 3 zum Begriff: Dies ist eine(r) der gemeinsamen Begriffe und Kerndefinitionen der harmonisierten Struktur für ISO-Managementsystemnormen. Die ursprüngliche Definition wurde durch Hinzufügen der Anmerkungen 1 und 2 zum Begriff abgeändert.

3.5

oberste Leitung

Person oder Personengruppe, die eine *Organisation* (3.2) auf der obersten Ebene führt und steuert

Anmerkung 1 zum Begriff: Die oberste Leitung ist innerhalb der Organisation in der Lage, Verantwortung zu delegieren und Ressourcen bereitzustellen.

Anmerkung 2 zum Begriff: Wenn der Anwendungsbereich des *Managementsystems* (3.1) nur einen Teil einer Organisation umfasst, bezieht sich „oberste Leitung“ auf diejenigen, die diesen Teil führen und steuern.

Anmerkung 3 zum Begriff: Dies ist eine(r) der gemeinsamen Begriffe und Kerndefinitionen der harmonisierten Struktur für ISO-Managementsystemnormen.

3.6

oberstes Organ

Person oder Gruppe von Personen mit der endgültigen *Verantwortlichkeit* (3.30) für die gesamte *Organisation* (3.2)

Anmerkung 1 zum Begriff: Jede organisatorische Einheit hat ein oberstes Organ, unabhängig davon, ob dieses ausdrücklich festgelegt ist oder nicht.

Anmerkung 2 zum Begriff: Ein oberstes Organ kann unter anderem einen Vorstand, Ausschüsse des Vorstands, einen Aufsichtsrat oder Treuhänder umfassen.

[QUELLE: ISO/IEC 38500:2015, 2.9, modifiziert — Die Worte „haben die endgültige Verantwortlichkeit“ wurden durch die Worte „sind verantwortlich für die Leistung und die Einhaltung von“ ersetzt und die Anmerkungen 1 und 2 zum Eintrag wurden hinzugefügt.]

3.7

Politik

Absichten und Ausrichtung einer *Organisation* (3.2) wie von der *obersten Leitung* (3.5) formell ausgedrückt

Anmerkung 1 zum Begriff: Dies ist eine(r) der gemeinsamen Begriffe und Kerndefinitionen der harmonisierten Struktur für ISO-Managementsystemnormen.

3.8

Fehlverhalten

Handlung(en) oder Unterlassung(en), die Schäden verursachen kann/können

Anmerkung 1 zum Begriff: Fehlverhalten kann Folgendes enthalten, ist aber nicht darauf begrenzt:

- Gesetzesverstöße (national oder international) wie Betrug, Korruption einschließlich Bestechung;
- Verstöße gegen den Verhaltenskodex der *Organisation* (3.2) oder einen anderen relevanten Verhaltenskodex, Verstöße gegen die *Politiken* (3.7) der Organisation;
- grobe Fahrlässigkeit, Mobbing, Belästigung, Diskriminierung, unbefugte Verwendung von Geldern oder Ressourcen, Amtsmissbrauch, Interessenkonflikte, grobe Verschwendung oder Misswirtschaft;
- Handlungen oder Unterlassungen, die zu einer Verletzung der Menschenrechte führen oder das Risiko einer Schädigung der Umwelt, der öffentlichen Gesundheit und Sicherheit, sicherer Arbeitspraktiken oder des öffentlichen Interesses bergen.

Anmerkung 2 zum Begriff: Ein Fehlverhalten oder die daraus folgende Schädigung kann in der Vergangenheit erfolgt sein, gegenwärtig bestehen oder zukünftig geschehen.

Anmerkung 3 zum Begriff: Der potenzielle Schaden kann unter Bezugnahme auf ein einzelnes Ereignis oder eine Reihe von Ereignissen bestimmt werden.

3.9

Hinweisgeber

Person, die mutmaßliches oder tatsächliches *Fehlverhalten* (3.8) meldet und die zum Zeitpunkt der Meldung die begründete Vermutung hat, dass die Informationen der Wahrheit entsprechen

Anmerkung 1 zum Begriff: Eine begründete Vermutung ist eine Vermutung, die eine Person aufgrund von Beobachtungen, Erfahrungen oder ihr bekannten Informationen hat und die auch eine andere Person unter den gleichen Umständen haben würde.

Anmerkung 2 zum Begriff: Beispiele für Hinweisgeber beinhalten, ohne darauf beschränkt zu sein:

- *Personal* (3.3) innerhalb einer *Organisation* (3.2);
- Personal innerhalb externer Parteien, einschließlich juristischer Personen, mit denen die Organisation irgendeine Form der Geschäftsbeziehung begründet hat oder zu begründen plant, unter anderem Klienten, Kunden, Gemeinschaftsunternehmen, Partner eines Gemeinschaftsunternehmens, Konsortialpartner, Ausgliederungsanbieter, Auftragnehmer, Unternehmensberater, Unterauftragnehmer, Lieferanten, Verkäufer, Berater, Makler, Vertreiber, Vertreter, Mittler und Investoren;
- andere Personen wie Gewerkschaftsvertreter;
- jedwede, in der Vergangenheit oder zukünftig in einer der in dieser Definition genannten Positionen tätige Person.

3.10

Hinweisgeben

Meldung vermuteten oder tatsächlichen *Fehlverhaltens* (3.8) durch einen *Hinweisgeber* (3.9)

Anmerkung 1 zum Begriff: Die Meldung von Fehlverhalten kann in mündlicher Form, persönlich, schriftlich oder in einem elektronischen oder digitalen Format erfolgen.

Anmerkung 2 zum Begriff: Es ist üblich, die folgende Unterscheidung zu treffen:

- offen Hinweise geben, bei denen der Hinweisgeber Informationen bekannt gibt, ohne seine Identität geheim zu halten oder die Auflage zu machen, dass seine Identität geheim gehalten wird;
- vertraulich Hinweise geben, bei denen die Identität des Hinweisgebers und alle Informationen, die ihn identifizieren können, dem Empfänger bekannt sind, aber ohne die Zustimmung des Hinweisgebers an niemanden weitergegeben werden, der sie nicht kennen muss, es sei denn, dies ist gesetzlich vorgeschrieben;
- anonym Hinweise geben, bei denen die Informationen erhalten werden, ohne dass der Hinweisgeber seine Identität preisgibt.

Anmerkung 3 zum Begriff: *Organisationen* (3.2) können einen alternativen Begriff wie „ansprechen“, „Bedenken äußern“ oder dergleichen verwenden.

3.11

Hinweismanagementfunktion

Person oder Personen mit der Verantwortlichkeit und Befugnis für den Betrieb des *Managementsystems* (3.1) für *Hinweisgeben* (3.10)

3.12

Triage

Bewertung der ursprünglichen Meldung von *Fehlverhalten* (3.8) zwecks Kategorisierung, Ergreifung vorläufiger Maßnahmen, Priorisierung und Zuweisung zur weiteren Bearbeitung

Anmerkung 1 zum Begriff: Die folgenden Faktoren können berücksichtigt werden: Wahrscheinlichkeit und Schwere der Auswirkung von Fehlverhalten oder vermuteten Fehlverhaltens auf *Personal* (3.3), *Organisation* (3.2) und *interessierte Partei* (3.4), einschließlich Reputations-, Finanz-, Umwelt-, Personen-, oder andere Schäden.

3.13

nachteilige Behandlung

angedrohte, beabsichtigte oder tatsächliche, direkte oder indirekte Handlung oder Unterlassung zum möglichen Schaden des *Hinweisgebers* (3.9) oder einer sonstigen relevanten *interessierten Partei* (3.4) im Zusammenhang mit *Hinweisgeben* (3.10)

Anmerkung 1 zum Begriff: Der Schaden beinhaltet negative Konsequenzen arbeitsbezogener oder persönlicher Art, einschließlich, ohne darauf beschränkt zu sein, Entlassung, Beurlaubung, Herabstufung, Versetzung, Änderung von Zuständigkeiten, Veränderung der Arbeitsbedingungen, negative Bewertung der *Leistung* (3.26), Disziplinarverfahren, Beschränkung der Aufstiegsmöglichkeiten, Verweigerung von Leistungen, Aufnahme in eine „schwarze Liste“, Ächtung, Rufschädigung, Offenlegung der Identität des Hinweisgebers, Zufügung finanziellen Schadens, straf- oder zivilrechtliche Schritte, Belästigung, Isolierung oder Zufügen jedweder anderen Form physischen oder psychologischen Schadens.

Anmerkung 2 zum Begriff: Nachteilige Behandlung schließt Vergeltungsmaßnahmen, Repressalien, Strafmaßnahmen, vorsätzliche Handlungen oder Unterlassungen ein, die wissentlich die Schädigung eines Hinweisgebers oder sonstiger relevanter Parteien betreiben oder in Kauf nehmen.

Anmerkung 3 zum Begriff: Nachteilige Behandlung schließt außerdem das Versäumnis ein, durch entsprechende Sorgfalt in jedem Schritt des Hinweismeldungs-Prozesses (3.27) eine Schädigung zu verhindern oder so gering wie möglich zu halten.

Anmerkung 4 zum Begriff: Handlungen zur Beschäftigung mit dem *Fehlverhalten* (3.8), der Leistung oder dem Management eines Hinweisgebers selbst, die unabhängig von dessen Rolle bei der Hinweismeldung sind, gelten für die Anwendung dieses Dokuments nicht als nachteilige Behandlung.

Anmerkung 5 zum Begriff: Zu den sonstigen relevanten interessierten Parteien können potenzielle oder vermutete Hinweisgeber, Verwandte, Geschäftspartner von Hinweisgebern, Personen, die einen Hinweisgeber unterstützt haben, sowie jedwede Personen zählen, die in einen Hinweismeldungsprozess einbezogen sind, einschließlich juristischer Personen.

3.14

Untersuchung

systematischer, unabhängiger und dokumentierter *Prozess* (3.27) zur Feststellung von Tatsachen und deren objektiver Auswertung, um zu bestimmen, ob und in welchem Ausmaß ein *Fehlverhalten* (3.8) aufgetreten ist, vorliegt oder wahrscheinlich auftreten wird

Anmerkung 1 zum Begriff: Bei einer Untersuchung kann es sich um eine interne oder eine externe Untersuchung handeln. Diese kann eine kombinierte Untersuchung sein.

Anmerkung 2 zum Begriff: Eine interne Untersuchung wird von der *Organisation* (3.2) selbst durchgeführt, oder von einer externen Seite in ihrem Auftrag.

Anmerkung 3 zum Begriff: Die Organisation kann auch von externen Parteien dazu verpflichtet werden, eine Untersuchung durchzuführen.

3.15

Audit

systematischer und unabhängiger *Prozess* (3.27) zum Erlangen von Nachweisen und zu deren objektiver Auswertung, um zu bestimmen, inwieweit Auditkriterien erfüllt sind

Anmerkung 1 zum Begriff: Ein Audit kann ein internes (Erstparteien-Audit) oder externes (Zweitparteien- oder Drittparteien-Audit) Audit sein und es kann ein kombiniertes Audit sein (Verbindung zweier oder mehrerer Disziplinen).

Anmerkung 2 zum Begriff: Ein internes Audit wird von der *Organisation* (3.2) selbst durchgeführt, oder von einer externen Seite in ihrem Auftrag.

Anmerkung 3 zum Begriff: „Auditnachweis“ und „Auditkriterium“ sind in ISO 19011 definiert.

Anmerkung 4 zum Begriff: Dies ist eine(r) der gemeinsamen Begriffe und Kerndefinitionen der harmonisierten Struktur für ISO-Managementsystemnormen.

3.16

Kompetenz

Fähigkeit, Wissen und Fertigkeiten anzuwenden, um beabsichtigte Ergebnisse zu erzielen

Anmerkung 1 zum Begriff: Dies ist eine(r) der gemeinsamen Begriffe und Kerndefinitionen der harmonisierten Struktur für ISO-Managementsystemnormen.

3.17

Konformität

Erfüllung einer *Anforderung* (3.28)

Anmerkung 1 zum Begriff: Dies ist eine(r) der gemeinsamen Begriffe und Kerndefinitionen der harmonisierten Struktur für ISO-Managementsystemnormen.

3.18

Nichtkonformität

Nichterfüllung einer *Anforderung* (3.28)

Anmerkung 1 zum Begriff: Dies ist eine(r) der gemeinsamen Begriffe und Kerndefinitionen der harmonisierten Struktur für ISO-Managementsystemnormen.