

DIN ISO 37002

ICS 03.100.01; 03.100.02; 03.100.70

Einsprüche bis 2020-09-03

Entwurf**Hinweismanagementsysteme –
Leitlinien (ISO/DIS 37002:2020);
Text Deutsch und Englisch**

Whistleblowing management systems –
Guidelines (ISO/DIS 37002:2020);
Text in German and English

Systèmes de management des alertes –
Lignes directrices (ISO/DIS 37002:2020);
Texte en allemand et anglais

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-07-03 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an info@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Organisationsprozesse (NAOrg), 10772 Berlin oder Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 80 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	16
4.1 Verstehen der Organisation und ihres Kontextes	16
4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien	16
4.3 Festlegen des Anwendungsbereichs des Hinweismanagementsystems	16
4.4 Hinweismanagementsystem	17
5 Führung	18
5.1 Führung und Verpflichtung	18
5.1.1 Oberstes Organ	18
5.2 Politik	19
5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation	20
5.3.1 Oberste Leitung und oberstes Organ	20
5.3.2 Hinweismanagementfunktion	21
5.3.3 Delegierte Entscheidungsfindung	21
6 Planung	22
6.1 Maßnahmen zum Umgang mit Risiken und Möglichkeiten	22
6.2 Ziele des Hinweismanagementsystems und Planung zu deren Erreichung	22
7 Unterstützung für das Hinweismanagementsystem	23
7.1 Ressourcen	23
7.2 Kompetenz	23
7.3 Bewusstsein und Schulung	24
7.3.1 Allgemeines	24
7.3.2 Personalschulung und Sensibilisierungsmaßnahmen	25
7.3.3 Schulung für die Führung und spezifische Rollen innerhalb des Hinweismanagementsystems	26
7.4 Kommunikation	26
7.5 Dokumentierte Information	27
7.5.1 Allgemeines	27
7.5.2 Erstellen und Aktualisieren	27
7.5.3 Lenkung dokumentierter Information	28
7.5.4 Datenschutz	28
7.5.5 Vertraulichkeit	29
8 Betrieb	29
8.1 Betriebliche Planung und Steuerung	29
8.2 Entgegennahme von Berichten über Fehlverhalten	31
8.3 Bewertung von Berichten über Fehlverhalten	33
8.3.1 Bewertung des gemeldeten Fehlverhaltens	33
8.3.2 Bewertung und Vorbeugung von Risiken nachteiliger Behandlung	34
8.4 Eingehen auf Berichte über Fehlverhalten	35
8.4.1 Eingehen auf gemeldetes Fehlverhalten	35
8.4.2 Schutz und Unterstützung des Hinweisgebers	36
8.4.3 Eingehen auf nachteilige Behandlung	36
8.4.4 Schutz der Person(en), die Gegenstand eines Berichts ist/sind	37
8.4.5 Schutz relevanter interessierter Parteien	37
8.5 Abschluss von Fällen aufgrund von Hinweisgebermeldungen	37

9	Bewertung der Leistung	38
9.1	Überwachung, Messung, Analyse und Bewertung	38
9.1.1	Allgemeines	38
9.1.2	Bewertungsindikatoren	39
9.1.3	Informationsquellen	40
9.2	Internes Audit	40
9.3	Managementbewertung	41
10	Verbesserung	41
10.1	Nichtkonformität und Korrekturmaßnahmen	41
10.2	Fortlaufende Verbesserung	42
	Literaturhinweise	43

Bilder

Bild 1	Übersicht eines Hinweismanagementsystems	9
Bild 2	Beziehung zwischen dem Hinweismanagementsystem und anderen Organisationsprozessen	17
Bild 3	Verfahrensschritte des Hinweismanagementsystems	31

Nationales Vorwort

Dieses Dokument enthält die deutsche Übersetzung der Internationalen Norm ISO/DIS 37002:2020, die vom Technischen Komitee ISO/TC 309 „Governance of organizations“ erarbeitet wurde, dessen Sekretariat von BSI (Vereinigtes Königreich) gehalten wird.

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

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

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

ISO 19011	siehe	DIN EN ISO 19011
ISO/IEC 27001	siehe	DIN EN ISO/IEC 27001
ISO/IEC 27018	siehe	DIN ISO/IEC 27018
ISO 31000	siehe	DIN ISO 31000
ISO 37001	siehe	DIN ISO 37001
ISO/DIS 37301	siehe	E 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 19011, *Leitfaden zur Auditierung von Managementsystemen*

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

DIN 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, *Managementsysteme zur Korruptionsbekämpfung — Anforderungen mit Leitlinien zur Anwendung*

E DIN ISO 37301, *Compliance-Managementsysteme — Anforderungen mit Anleitung 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.

Rückmeldungen 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 Hinweisgebermeldungen 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 Berichte von Personen bekannt werden, die innerhalb der Organisation tätig sind oder eng mit dieser zusammenarbeiten.

Organisationen gehen immer mehr dazu über, als Reaktion auf behördliche Vorgaben oder auf freiwilliger Basis Politiken und Prozesse für interne Hinweisgebermeldungen einzuführen.

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

- a) Förderung und Erleichterung der Meldung von Fehlverhalten;
- b) Unterstützung und Schutz von Hinweisgebern und anderer beteiligter Personen;
- c) Sicherstellung, dass Berichten über Fehlverhalten ordnungsgemäß und zeitnah nachgegangen wird;
- d) Verbesserung der Organisationskultur, Governance und vorbeugenden Maßnahmen gegen Fehlverhalten.

Zu den potenziellen Vorteilen für die Organisation gehören:

- Möglichkeit für die Organisation, Fehlverhalten frühzeitig zu erkennen und darauf einzugehen,
- um zur Verhinderung oder Minimierung des Verlusts von Assets beizutragen und bei der Wiedererlangung verlorener Assets zu helfen;
- um die Einhaltung der Politiken und Verfahren der Organisation sowie der gesetzlichen und sozialen Verpflichtungen sicherzustellen;
- um Personal zu gewinnen und zu halten, das sich den Werten der Organisation und der Organisationskultur verpflichtet fühlt sowie
- um der Gesellschaft, den Märkten, den Aufsichtsbehörden, den Eigentümern und anderen interessierten Partei die Einhaltung fundierter ethischer Governancepraktiken zu demonstrieren.

Ein wirksames Hinweismanagementsystem schafft Vertrauen in die Organisation, indem:

- die Führung ihre Entschlossenheit zeigt, Fehlverhalten zu verhindern bzw. darauf einzugehen;
- 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 und Verantwortlichkeit zu fördern.

Dieses Dokument gibt Organisationen Leitlinien für die Schaffung eines Hinweismanagementsystems auf Basis der Grundsätze 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 Politiken und Verfahren für Hinweisgebermeldungen zu verbessern oder die Einhaltung der geltenden Gesetzgebung zu Hinweisgebermeldungen zu gewährleisten.

Dieses Dokument wendet die „High-Level-Structure“ an (d. h. feste Abschnittsreihenfolge, einheitlicher Text und einheitliche Terminologie), die von der ISO erarbeitet wurde, um die Internationalen Normen für Manage-

mentssysteme anzugleichen. Organisationen können dieses Dokument als eigenständige Leitlinie auf ihre Organisation oder neben anderen Managementsystem-Normen anwenden, unter anderem um auf Hinweisgebermeldungen betreffende Anforderungen in anderen Managementsystemen einzugehen.

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

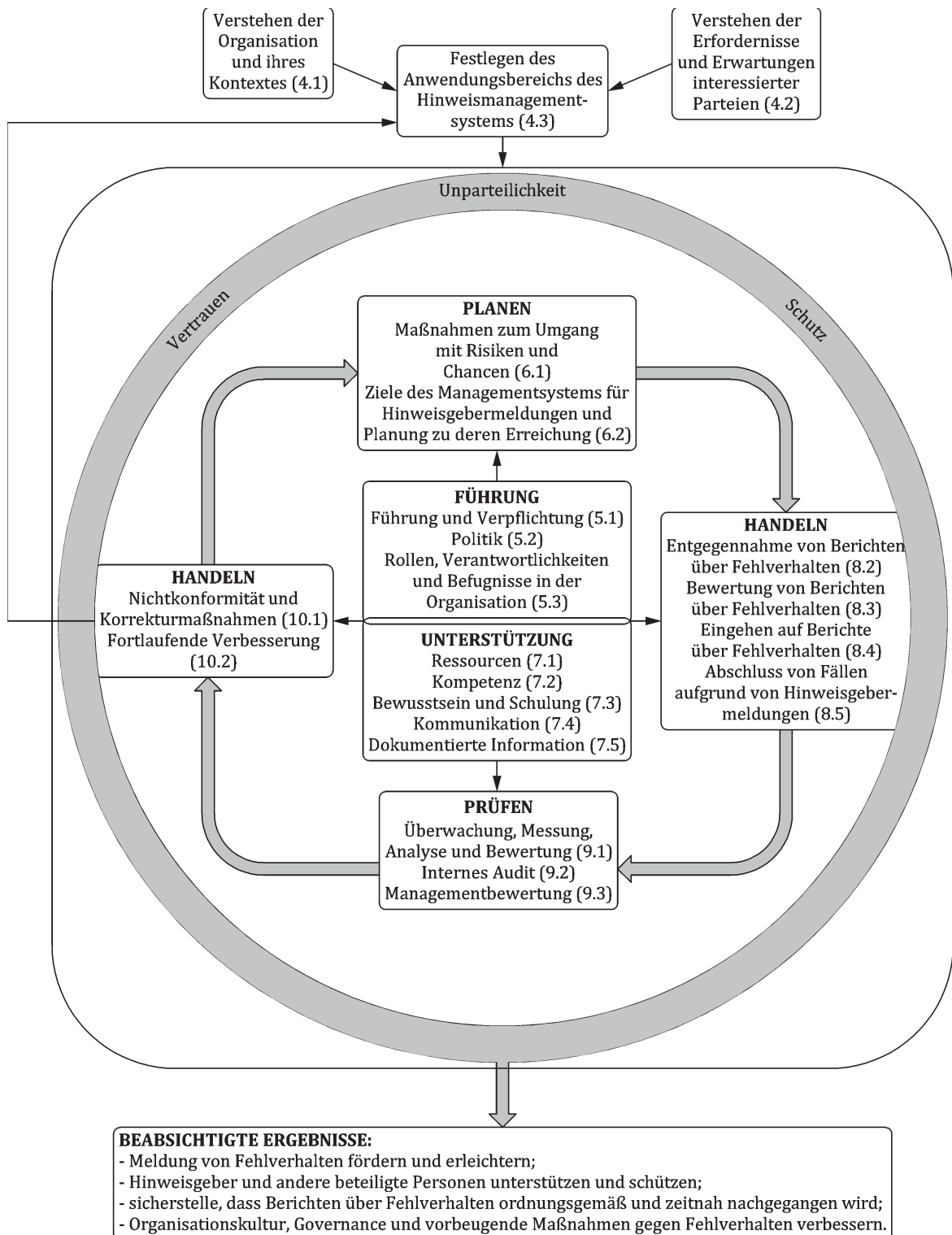


Bild 1 — Übersicht eines Hinweismanagementsystems

1 Anwendungsbereich

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

- a) Entgegennahme von Berichten über Fehlverhalten;
- b) Bewertung von Berichten über Fehlverhalten;
- c) Eingehen auf Berichte über Fehlverhalten;
- d) Abschluss von Fällen aufgrund von Hinweisgebermeldungen.

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.

Das Ausmaß der Anwendung dieses Leitfadens hängt von den in 4.1, 4.2 und 4.3 festgelegten Faktoren ab. Das System kann eigenständig oder in ein gesamtes 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>
- IEC Electropedia: verfügbar unter <http://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* (3.12) zum Erreichen dieser Ziele festzulegen

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

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

Anmerkung 3 zum Begriff: Der Anwendungsbereich eines Managementsystems kann die ganze Organisation, bestimmte Funktionen der Organisation, bestimmte Bereiche der Organisation oder eine oder mehrere Funktionen über eine Gruppe von Organisationen hinweg umfassen.

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.

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, modifiziert durch Streichung der Anmerkungen zum Begriff]

3.4

interessierte Partei (bevorzugte Benennung)

Anspruchsgruppe (zulässige Benennung)

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

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

Anmerkung 2 zum Begriff: Zu den Anspruchsgruppen können unter anderem Personen gehören, die Bericht erstatten, Personen, die Gegenstand dieser Meldungen sind, Zeugen, Mitarbeiter, Arbeitnehmervertreter, Lieferanten, Dritte, die Öffentlichkeit, Medien, Aufsichtsbehörden und die Organisation als Ganzes.

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 der Organisation umfasst, bezieht sich „oberste Leitung“ auf diejenigen, die diesen Teil führen und steuern.

3.6

oberstes Organ

Person oder Gruppe von Personen mit der endgültigen Verantwortlichkeit und Befugnis für die Aktivitäten, Führung und Politiken einer *Organisation* (3.2), und der/dem die *oberste Leitung* (3.5) berichtet und der/dem gegenüber die oberste Leitung Rechenschaft ablegt

Anmerkung 1 zum Begriff: Nicht alle Organisationen, insbesondere kleine Organisationen, haben ein von der *obersten Leitung* separates oberstes Organ.

Anmerkung 2 zum Begriff: Ein oberstes Organ können unter anderem ein Verwaltungsrat, Ausschüsse des Verwaltungsrats, ein Aufsichtsrat, Treuhänder oder Aufseher sein.

[QUELLE: ISO/IEC 38500:2015, 2.9 geändert]

3.7

Politik

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

3.8

Fehlverhalten

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

Anmerkung 1 zum Begriff: Fehlverhalten kann unter anderem Folgendes umfassen: unethisches Verhalten, Betrug, Korruption und Bestechung, Verstoß gegen (national oder internationales) Recht, Verstoß gegen den Verhaltenskodex der Organisation oder einen sonstigen relevanten Verhaltenskodex, grobe Fahrlässigkeit, Verstoß gegen die Politik der Organi-

sation, Diskriminierung, Mobbing, unberechtigte Verwendung öffentlicher Mittel oder Ressourcen, Autoritätsmissbrauch, Interessenkonflikt, Verschwendung oder Misswirtschaft.

Anmerkung 2 zum Begriff: Fehlverhalten kann außerdem Handlungen oder Unterlassungen umfassen, 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 3 zum Begriff: Ein Fehlverhalten oder die Schädigung kann in der Vergangenheit erfolgt sein, gegenwärtig bestehen oder eine zukünftige Möglichkeit darstellen.

Anmerkung 4 zum Begriff: Der potenzielle Schaden kann unter Bezugnahme auf ein einzelnes Ereignis oder eine Reihe von Ereignissen bestimmt werden.

3.9

Hinweisgeber

Person, die Fehlverhalten (3.8) meldet

3.10

Hinweisgebermeldungen

Meldung von Fehlverhalten (3.8) durch einen Hinweisgeber (3.9), der stichhaltige Gründe für die Annahme hat, dass die gemeldeten Informationen zum Zeitpunkt der Meldung der Wahrheit entsprechen

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:

- offene Hinweisgebermeldungen: Hinweisgeber gibt Informationen bekannt, ohne seine Identität geheimzuhalten oder die Auflage zu machen, dass seine Identität geheimgehalten wird.
- vertrauliche Hinweisgebermeldungen: Die Identität des Hinweisgebers und jedwede Informationen, die Rückschlüsse auf seine Person zulassen, sind dem Empfänger bekannt, werden jedoch ohne Zustimmung des Hinweisgebers nicht bekanntgegeben, es sei denn, dass dies gesetzlich und/oder für den Untersuchungsprozess erforderlich ist.
- anonyme Hinweisgebermeldungen: Die Informationen werden erhalten, ohne dass der Hinweisgeber seine Identität preisgibt.

Anmerkung 3 zum Begriff: Organisationen dürfen nach Wunsch 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 *Hinweismanagementsystems* (3.1).

3.12

Sichtung

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

Anmerkung 1 zum Begriff: Die folgenden Faktoren können berücksichtigt werden: Wahrscheinlichkeit und Schwere der Auswirkung von Fehlverhalten auf Personal (3.3), *Organisation* (3.2) und *interessierte Parteien* (3.4), einschließlich Schaden für Ansehen, Finanzen, Umwelt, Menschen oder andere Schäden.

3.13

Nachteilige Behandlung

jedwede angedrohte, beabsichtigte oder tatsächliche, direkte oder indirekte Handlung oder Unterlassung zum möglichen Schaden des Hinweisgebers (3.9) oder einer sonstigen relevanten Partei im Zusammenhang mit der Meldung von Fehlverhalten (3.8)

Anmerkung 1 zum Begriff: Der Schaden kann negative Konsequenzen arbeitsbezogener oder persönlicher Art einschließen, darunter Entlassung, Beurlaubung, Herabstufung, Versetzung, Änderung von Zuständigkeiten, Veränderung der Arbeitsbedingungen, negative Leistungsbewertungen, Beschränkung der Aufstiegsmöglichkeiten, Verweigerung von Leistungen, Aufnahme in eine „schwarze Liste“, Ächtung, Rufschädigung, Zufügung finanziellen Schadens, straf- oder zivilrechtliche Schritte, Belästigung, Isolierung oder jedwede andere 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 Hinweismeldungsprozesses eine Schädigung zu verhindern oder so gering wie möglich zu halten.

Anmerkung 4 zum Begriff: Zu den sonstigen relevanten interessierten Parteien können potenzielle oder als solche wahrgenommene Hinweisgeber, Verwandte, Geschäftspartner von Personen, die einen Hinweisgeber unterstützt haben, sowie jedwede Personen zählen, die in einen Hinweismeldungsprozess einbezogen sind, einschließlich juristischer Personen.

Anmerkung 5 zum Begriff: Handlungen zur Beschäftigung mit dem Fehlverhalten, 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. Jedoch sind derartige Handlungen von den Umständen der Meldung und den Grundsätzen Vertrauen, Unparteilichkeit und Schutz abhängig, die die Basis des Hinweismanagementsystems darstellen.

3.14

Untersuchung

systematischer, unabhängiger und dokumentierter *Prozess* (3.28) zur Erlangung von Nachweisen und deren objektiver Auswertung, um zu bestimmen, ob und in welchem Ausmaß ein Fehlverhalten vorliegt

Anmerkung 1 zum Begriff: Bei einer Untersuchung kann es sich um eine interne oder eine externe Untersuchung handeln, und es kann eine kombinierte Untersuchung stattfinden.

Anmerkung 2 zum Begriff: Eine interne Untersuchung wird von der Organisation selbst durchgeführt, oder von einer externen Stelle in ihrem Auftrag.

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

3.15

Audit

systematischer, unabhängiger und dokumentierter *Prozess* (3.28) zum Erlangen von Auditnachweisen und zu deren objektiver Auswertung, um zu bestimmen, inwieweit Auditkriterien erfüllt sind

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

Anmerkung 2 zum Begriff: Ein internes Audit wird von der Organisation selbst durchgeführt, oder von einer externen Stelle in ihrem Auftrag.

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

3.16

Kompetenz

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

3.17

Konformität

Erfüllung einer *Anforderung* (3.29)

3.18

Nichtkonformität

Nichterfüllung einer *Anforderung* (3.29)

3.19

Korrekturmaßnahme

Maßnahme zum Beseitigen der Ursache einer *Nichtkonformität* (3.18) und zum Verhindern des erneuten Auftretens

3.20

fortlaufende Verbesserung

wiederkehrende Tätigkeit zum Steigern der *Leistung* (3.27)

3.21

dokumentierte Information

Information, die von einer *Organisation* (3.2) gelenkt und aufrechterhalten werden muss, und das Medium, auf dem sie enthalten ist

Anmerkung 1 zum Begriff: Dokumentierte Information kann in jeglichem Format oder Medium vorliegen sowie aus jeglicher Quelle stammen.

Anmerkung 2 zum Begriff: Dokumentierte Information kann sich beziehen auf:

- Das *Managementsystem* (3.1), einschließlich damit verbundener *Prozesse* (3.28);
- Informationen, die für den Betrieb der Organisation geschaffen wurden (Dokumentation);
- Nachweise erreichter Ergebnisse (Aufzeichnungen).

3.22

Wirksamkeit

Ausmaß, in dem geplante Tätigkeiten verwirklicht und geplante Ergebnisse erreicht werden

3.23

Messung

Prozess (3.28) zum Bestimmen eines Wertes

3.24

Überwachung

Bestimmung des Zustands eines Systems, eines *Prozesses* (3.18) oder einer Tätigkeit

Anmerkung 1 zum Begriff: Zur Bestimmung des Zustands kann es erforderlich sein, zu prüfen, zu beaufsichtigen oder kritisch zu beobachten.

3.25

Ziel

zu erreichendes Ergebnis

Anmerkung 1 zum Begriff: Ein Ziel kann strategisch, taktisch oder operativ sein.

Anmerkung 2 zum Begriff: Ziele können sich auf verschiedene Disziplinen beziehen (z. B. finanzielle, gesundheits- und sicherheitsbezogene sowie umweltbezogene Ziele) und für verschiedene Ebenen gelten (z. B. strategisch, organisationsweit, projekt-, produkt-, prozessbezogen (3.28)).

Anmerkung 3 zum Begriff: Eine Zielsetzung kann anderweitig ausgedrückt werden, z. B. als beabsichtigtes Ergebnis, Zweck, betriebstechnisches Kriterium, als Zielsetzung der Hinweisgebermeldung oder durch Verwendung anderer Worte mit ähnlicher Bedeutung (z. B. Zielvorgabe, Zielstellung oder Einzelziel).

Anmerkung 4 zum Begriff: Im Zusammenhang mit Hinweismanagementsystemen werden zum Erreichen bestimmter Ergebnisse Zielsetzungen der Hinweisgebermeldung durch die Organisation in Übereinstimmung mit deren Politik zu Hinweisgebermeldungen festgelegt.

3.26

ausgliedern

eine Vereinbarung treffen, bei der eine externe *Organisation* (3.2) einen Teil einer Funktion oder eines *Prozesses* (3.28) einer Organisation wahrnimmt bzw. durchführt

Anmerkung 1 zum Begriff: Eine externe Organisation befindet sich außerhalb des Anwendungsbereichs des *Managementsystems* (3.1), obwohl die ausgegliederte Funktion oder der ausgegliederte Prozess im Rahmen des Anwendungsbereichs liegen.

3.27

Leistung

messbares Ergebnis

Anmerkung 1 zum Begriff: Leistung kann sich auf quantitative oder qualitative Feststellungen beziehen.

Anmerkung 2 zum Begriff: Leistung kann sich auf das Führen und Steuern von Tätigkeiten, *Prozessen* (3.28), Produkten (einschließlich Dienstleistungen), Systemen oder *Organisationen* (3.2) beziehen.

3.28

Prozess

Satz zusammenhängender oder sich gegenseitig beeinflussender Tätigkeiten, der Eingaben in Ergebnisse umwandelt

3.29

Anforderung

Erfordernis oder Erwartung, das oder die festgelegt, üblicherweise vorausgesetzt oder verpflichtend ist

Anmerkung 1 zum Begriff: „Üblicherweise vorausgesetzt“ bedeutet, dass es für die Organisation und andere interessierte Parteien übliche oder allgemeine Praxis ist, dass das entsprechende Erfordernis oder die entsprechende Erwartung vorausgesetzt wird.

Anmerkung 2 zum Begriff: Eine festgelegte Anforderung ist eine, die z. B. in dokumentierter Information enthalten ist.

3.30

Risiko

Auswirkung von Unsicherheit auf Ziele

Anmerkung 1 zum Begriff: Eine Auswirkung ist eine Abweichung vom Erwarteten — in positiver oder negativer Hinsicht.

Anmerkung 2 zum Begriff: Ungewissheit ist der Zustand des, auch teilweisen, Fehlens von Informationen im Hinblick auf das Verständnis eines Ereignisses oder Wissen über ein Ereignis, seine Folgen oder seine Wahrscheinlichkeit.

Anmerkung 3 zum Begriff: Risiko wird häufig durch Bezugnahme auf mögliche „Ereignisse“ (definiert in ISO Guide 73) und „Folgen“ (definiert in ISO Guide 73), oder durch eine Kombination beider charakterisiert.

Anmerkung 4 zum Begriff: Risiko wird häufig mittels der Folgen eines Ereignisses (einschließlich Veränderungen der Umstände) in Verbindung mit der „Wahrscheinlichkeit“ (definiert in ISO Guide 73) seines Eintretens beschrieben.

3.31

Zurechenbarkeit

Eigenschaft, die gewährleistet, dass Aktionen einer Instanz auch auf diese zurückgeführt werden können

4 Kontext der Organisation

4.1 Verstehen der Organisation und ihres Kontextes

Die Organisation sollte externe und interne Themen bestimmen, die für ihren Zweck relevant sind und sich auf ihre Fähigkeit auswirken, die beabsichtigten Ergebnisse ihres Hinweismanagementsystems zu erreichen.

Diese Themen können die folgenden Punkte umfassen, sind jedoch nicht darauf beschränkt:

- a) die Größe und Struktur;
- b) die Standorte und Sektoren an bzw. in denen die Organisation tätig ist oder erwartet, tätig zu werden;
- c) die Beschaffenheit, Kultur, der Umfang und die Komplexität der Tätigkeiten und Betriebsabläufe der Organisation;
- d) die Beschaffenheit und Bedürfnisse des Personals;
- e) das Geschäftsmodell der Organisation;
- f) die von der Organisation kontrollierten Organisationen und die Organisationen, die Kontrolle über die Organisation ausüben, einschließlich des/der wirtschaftlichen Eigentümer(s) der Organisation;
- g) die Geschäftspartner der Organisation;
- h) das öffentliche Interesse, mit dem Organisation konfrontiert ist; sowie
- i) zutreffende gesetzliche, regulatorische, vertragliche und berufliche Verpflichtungen und Aufgaben.

ANMERKUNG Eine Organisation kontrolliert eine andere Organisation, wenn sie direkt oder indirekt die Leitung der anderen Organisation kontrolliert.

4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien

Die Organisation sollte bestimmen:

- die interessierten Parteien, die für ihr Hinweismanagementsystem relevant sind;
- die relevanten Anforderungen dieser interessierten Parteien.

4.3 Festlegen des Anwendungsbereichs des Hinweismanagementsystems

Die Organisation sollte die Grenzen und die Anwendbarkeit des Hinweismanagementsystems bestimmen, um dessen Anwendungsbereich festzulegen.

Bei der Festlegung dieses Anwendungsbereichs sollte die Organisation Folgendes berücksichtigen:

- die unter 4.1 genannten externen und internen Themen;
- die unter 4.2 genannten Empfehlungen;
- wer (interne / externe interessierte Parteien) von wo aus (Regionen / Geographie) Meldung erstatten kann und welche Arten von Fehlverhalten von dem System abgedeckt werden, siehe Bild 2;
- die Ergebnisse Compliance-Risikobeurteilungen oder vergleichbarer Daten, je nach Verfügbarkeit;

ANMERKUNG 1 Organisationen können für die Compliance-Risikobeurteilung auf ISO 37301 und für das Risikomanagement auf ISO 31000 verweisen.

ANMERKUNG 2 Beispiele für Hinweisgeber sind unter anderem:

- Personal innerhalb einer Organisation (3.2);
- Externe Partei, einschließlich juristischer Personen, mit denen die Organisation (3.2) irgendeine Form der Geschäftsbeziehung unterhält 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;
- sonstige Personen wie verbundene Personen und Gewerkschaftsvertreter sowie
- jedwede, in der Vergangenheit oder zukünftig in einer der in dieser Definition genannten Positionen tätige Person.

Zur Bestimmung des Anwendungsbereichs des Hinweismanagementsystems ist es besonders wichtig festzuhalten, welche Arten von Fehlverhalten (siehe 3.8) dazu führen, dass das Managementsystem tätig wird. Auch wenn das Hinweismanagementsystem nicht tätig wird, oder wenn in Meldungen verschiedene Arten von Fehlverhalten geschildert werden, sollte die Organisation ermitteln und berücksichtigen, welche anderen bestehenden oder geplanten Prozesse angewendet werden könnten, um Meldungen (z. B. Beanstandungen und Beschwerden) nachzugehen und wie dies koordiniert werden könnte. Dies ist in Bild 2 dargestellt.

Der Anwendungsbereich sollte als dokumentierte Information verfügbar sein.

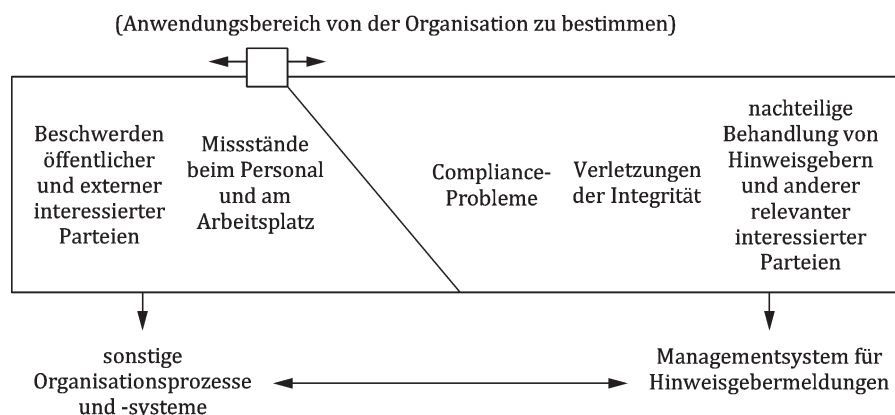


Bild 2 — Beziehung zwischen dem Hinweismanagementsystem und anderen Organisationsprozessen

4.4 Hinweismanagementsystem

Die Organisation sollte entsprechend der Anleitung in diesem Dokument ein Hinweismanagementsystem aufbauen, verwirklichen, aufrechterhalten und fortlaufend verbessern, einschließlich der benötigten Prozesse und ihrer Wechselwirkungen.

Das Hinweismanagementsystem sollte über den gesamten Prozess sollte die Grundsätze Vertrauen, Unparteilichkeit und Schutz anwenden und für entsprechende Rückmeldung sorgen. Das Hinweismanagementsystem sollte sämtliche Schritte des Hinweismeldungsprozesses unterstützen:

- a) **Entgegennahme von Berichten über Fehlverhalten:** Das Hinweismanagementsystem sollte festlegen, wie Meldungen erfolgen und entgegengenommen werden können, unter Berücksichtigung der in 4.3 genannten Faktoren.

- b) **Bewertung von Berichten über Fehlverhalten (Sichtung):** Das Hinweismanagementsystem sollte den Prozess für die Bewertung der entgegengenommenen Berichte festlegen, unter Einbeziehung von Aspekten wie: Priorität, Vollständigkeit und Relevanz der Informationen. Gleichzeitig sollte das Hinweismanagementsystem für die Bewertung des Risikos persönlicher Nachteile und des erforderlichen Schutzes für Hinweisgeber und andere Beteiligte sorgen.
- c) **Eingehen auf Berichte über Fehlverhalten:** Das Hinweismanagementsystem sollte für eine unparteiische und zeitnahe Untersuchung sorgen sowie für wirksame und zeitnahe Schutzmaßnahmen und ggf. Überwachung für den Hinweisgeber und jene, die Gegenstand des Berichts sind. Diese Schutzmaßnahmen können zur Verhinderung und Begrenzung sowie zur Behebung nachteiliger Auswirkungen führen.
- d) **Abschluss von Fällen aufgrund von Hinweisgebermeldungen:** Das Hinweismanagementsystem sollte einen Mechanismus bereithalten, um Untersuchungen abzuschließen sowie Empfehlungen und Entscheidungen auf Grundlage der Ergebnisse des Schrittes zum Eingehen auf die Berichte formulieren. Außerdem sollte sichergestellt werden, dass Schutzmaßnahmen fortgesetzt werden können und ggf. überwacht werden. Die Ergebnisse können für die Management-Berichterstattung, für organisatorisches Lernen und andere Maßnahmen (d. h. Behebungsmaßnahmen zur Minderung) verwendet werden.

Die Schritte des Hinweismeldungsprozesses sind in 8.2 bis 8.5 festgelegt.

5 Führung

5.1 Führung und Verpflichtung

5.1.1 Oberstes Organ

Das oberste Organ sollte:

- a) Ziele festlegen und die oberste Leitung hinsichtlich eines wirksamen Hinweismanagementsystems überwachen;
- b) die Unternehmenspolitik bezüglich Hinweisgebermeldungen genehmigen und deutliche Botschaften bezüglich ihrer Existenz und Anwendung vermitteln;
- c) dieses Engagement durch positive Begleitung der Politik und des Hinweismanagementsystems demonstrieren;
- d) in geplanten Abständen Informationen über den Inhalt und den Betrieb des Hinweismanagementsystems der Organisation erhalten und überprüfen;
- e) sicherstellen, dass angemessene und geeignete Ressourcen, die für den wirksamen Betrieb des Hinweismanagementsystems notwendig sind, zugewiesen und zugeteilt werden, sowie
- f) eine angemessene Aufsichtsfunktion bezüglich der Umsetzung, Integrität und Verbesserung des Hinweismanagementsystems der Organisation wahrnehmen.

Oberste Leitung

Die oberste Leitung sollte in Bezug auf das Hinweismanagementsystem Führung und Verpflichtung zeigen, indem sie:

- sicherstellt, dass die Politik zu Hinweisgebermeldungen und die Ziele des Hinweismanagementsystems festgelegt und mit den Werten, Zielen und der strategischen Ausrichtung der Organisation vereinbar sind;
- die Politik zu Hinweisgebermeldungen der Organisation genehmigt;
- die Zugänglichkeit des Hinweismanagementsystems sicherstellt und zu dessen Nutzung ermutigt;

- sicherstellt, dass die Empfehlungen des Hinweismanagementsystems in die Geschäftsprozesse der Organisation, einschließlich der Managementsysteme, integriert werden;
- sicherstellt, dass die für das Hinweismanagementsystem erforderlichen Ressourcen zur Verfügung stehen sowie ausreichend, angemessen und einsatzbereit sind;
- die Bedeutung eines wirksamen Hinweismanagementsystems sowie die Wichtigkeit der Erfüllung der Anforderungen des Hinweismanagementsystems vermittelt;
- die Politik zu Hinweisgebermeldungen nach innen und außen kommuniziert;
- sicherstellt, dass das Hinweismanagementsystem sein beabsichtigtes Ergebnis bzw. seine beabsichtigten Ergebnisse erzielt, siehe 6.1; Personen anleitet und unterstützt, damit diese zur Wirksamkeit des Hinweismanagementsystems beitragen können;
- fortlaufende Verbesserung fördert;
- andere relevante Führungskräfte unterstützt, um deren Führungsrolle in deren jeweiligen Verantwortungsbereichen deutlich zu machen;
- innerhalb der Organisation eine Kultur des Ansprechens und Zuhörens fördert und praktiziert;
- sicherstellt, dass Hinweisgeber und sonstige Beteiligte seitens der Organisation im Zusammenhang mit der Hinweismeldung keine Nachteile erleiden; in geplanten Abständen Berichte zum Betrieb und zur Leistung des Hinweismanagementsystems entgegennimmt und überprüft, sowie
- sicherstellt, dass eine unparteiische Untersuchung der mittels des Systems gemeldeten Angelegenheiten erfolgt, ungeachtet der Identität des Hinweisgebers, des Gegenstands der Meldung und der Auswirkungen der festgestellten Themen.

ANMERKUNG 1 Wenn in diesem Dokument das Wort „Geschäft“ (en: business) verwendet wird, ist dieses im weiteren Sinne zu verstehen und bezieht sich auf Tätigkeiten, die für den Zweck der Organisation bzw. deren Existenz entscheidend sind.

ANMERKUNG 2 Eine Kultur des Ansprechens und Zuhörens ist als eine von einem vertrauenswürdigen Dialog geprägte Umgebung zu verstehen, in der sich alle relevanten Parteien ausreichend sicher und bestärkt fühlen, Fehlverhalten oder vermutetes Fehlverhalten zu melden, und die Organisation ihr Engagement demonstriert, Meldungen von Hinweisgebern entgegenzunehmen, zu bewerten, nachzugehen und die sich daraus ergebenden Fällen zum Abschluss zu bringen.

Die Vertrauenswürdigkeit des Hinweismanagementsystems hängt davon ab, inwieweit die interessierten Parteien wahrnehmen, dass sich die Leitung für das System einsetzt und bereit ist, die entsprechenden Verfahren anzuwenden.

5.2 Politik

Die oberste Leitung sollte eine Politik zu Hinweisgebermeldungen festlegen, die:

- a) für den Zweck der Organisation angemessen ist;
- b) einen Rahmen zum Festlegen von Zielen des Hinweismanagementsystems bietet;
- c) den Anwendungsbereich des Hinweismanagementsystems erläutert (siehe 4.3);
- d) eine Verpflichtung zur Erfüllung zutreffender Anforderungen enthält,
- e) eine Verpflichtung zur fortlaufenden Verbesserung des Hinweismanagementsystems enthält;

- f) nachteilige Behandlung verbietet;
- g) ein deutliches Bekenntnis zur Kultur des Ansprechens und Zuhörens beinhaltet;
- h) in leicht verständlicher Sprache eine Anleitung zur Meldung von Hinweisen bietet;
- i) eine Bekenntnis zu Vertrauen, Unparteilichkeit und Schutz über den gesamten Hinweismeldungsprozess enthält;
- j) für die Wahrung der Vertraulichkeit bei der Meldung von Fehlverhalten sorgt;
- k) die Befugnis und Unabhängigkeit der Hinweismanagementfunktion erklärt;
- l) die Konsequenzen bei Nichtbeachtung der Politik zu Hinweisgebermeldungen erläutert, z. B. kann die Abgabe wissentlich falscher Meldungen oder die nachteilige Behandlung von Hinweisgebern zur Einleitung von Disziplinarmaßnahmen führen;
- m) auf alternative Meldewege verweist, die außerhalb der Organisation zur Verfügung stehen, z. B. Aufsichtsbehörden;
- n) auf geltendes Recht verweist;
- o) wichtige Schritte des Untersuchungsprozesses umreißt, einschließlich der Art und Weise, die Meldungen entgegengenommen und abschließend bearbeitet werden;
- p) die Meldung nicht auf Grundlage vertraglicher Verpflichtungen, z. B. Verschwiegenheitserklärungen oder Klauseln zu firmenvertraulichen Daten oder Verschwiegenheitspflichten der Mitarbeiter usw. beschränkt.

Die Politik zu Hinweisgebermeldungen sollte:

- unter Mitwirkung des Personals und ggf. anderer interessierter Parteien erarbeitet werden;
- im Einklang mit anderen Politiken der Organisation stehen;
- direkt als dokumentierte Information verfügbar sein;
- regelmäßig in entsprechenden Sprachen innerhalb und außerhalb der Organisation bekanntgemacht werden;
- für interessierte Parteien verfügbar sein, ggf. unter entsprechender Berücksichtigung von Aspekten wie Alter, Sprache, Behinderungen usw., sowie
- regelmäßig überprüft werden.

5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation

5.3.1 Oberste Leitung und oberstes Organ

Die oberste Leitung sollte sicherstellen, dass die Verantwortlichkeiten und Befugnisse für relevante Rollen zugewiesen und innerhalb der Organisation bekannt gemacht werden.

Die oberste Leitung sollte die Verantwortlichkeit und Befugnis bezüglich der Hinweismanagementfunktion zuweisen für:

- a) das Sicherstellen, dass das Hinweismanagementsystem der Anleitung in diesem Dokument entspricht;
- b) das Berichten an die oberste Leitung über die Leistung des Hinweismanagementsystems.

Die oberste Leitung kann einzelne oder alle Hinweismanagementfunktionen an Personen außerhalb der Organisation zuweisen. In diesem Fall sollte die oberste Leitung sicherstellen, dass entsprechend bestimmtes Personal innerhalb der Organisation die Verantwortlichkeit für und Befugnis über diese extern zugewiesenen Teile der Funktion innehat.

Das oberste Organ, die oberste Leitung und das gesamte weitere Personal sollten dafür verantwortlich sein, die Anforderungen an das Hinweismanagementsystem zu verstehen, einzuhalten und anzuwenden, soweit diese ihre Rolle in der Organisation betreffen.

5.3.2 Hinweismanagementfunktion

Die Hinweismanagementfunktion sollte die Verantwortlichkeit und Befugnis innehaben für:

- a) Gestaltung, Umsetzung, Betrieb und Verbesserung des Hinweismanagementsystems;
- b) die Sicherstellung, dass das Hinweismanagementsystem so ausgelegt und mit Ressourcen ausgestattet ist, dass die umfassende Bewertung der Meldungen und der Risiken von Nachteilen für den Hinweisgeber, unparteiische und zeitnahe Untersuchungen der Meldungen sowie Vorkehrungen für Schutz und Unterstützung der Hinweisgeber gewährleistet sind;
- c) die Sicherstellung, im maximalen für die Organisation möglichen Ausmaß, dass die Untersuchungs- und Schutzfunktionen unabhängig voneinander bereitgestellt werden (d. h. von unterschiedlichen Personen oder Bereichen), wobei anzuerkennen ist, dass jede dieser Funktionen bestehenden Funktionen zugewiesen werden darf;
- d) die Bereitstellung von Beratung und Anleitung zum Hinweismanagementsystem und zu Themen im Zusammenhang mit der Meldung von Fehlverhalten;
- e) die Sicherstellung, dass das Hinweismanagementsystem der Anleitung in diesem Dokument entspricht;
- f) die geplante und auf Ad-hoc-Basis erfolgende Berichterstattung über die Leistung des Hinweismanagementsystems an das oberste Organ, die oberste Leitung und ggf. andere relevante Funktionen wie die Compliance-Funktion.

Die Hinweismanagementfunktion sollte angemessen ausgestattet (7.1) und Personal zugewiesen sein, das über angemessene Kompetenz, Integrität, Befugnis und Unabhängigkeit verfügt.

Die Hinweismanagementfunktion sollte über einen direkten, unbeschränkten und vertraulichen Zugang zur obersten Leitung und zum obersten Organ verfügen.

ANMERKUNG Organisationen, die über keine ausschließlich mit dieser Funktion betrauten Person verfügen, können eine Person oder mehrere Personen benennen, die diese Funktion zusätzlich zu anderen Verantwortlichkeiten ausfüllt bzw. ausfüllen, solange keine Interessenkonflikte oder Probleme bezüglich Vertrauenswürdigkeit oder Unparteilichkeit bestehen.

5.3.3 Delegierte Entscheidungsfindung

Die oberste Leitung kann die Befugnis für Entscheidungen im Rahmen des Hinweismeldungsprozesses, wie die Entgegennahme von Meldungen über Fehlverhalten, die Durchführung von Bewertungen, die Umsetzung von Schutzmaßnahmen, die Durchführung von Untersuchungen und den Abschluss der Fälle, delegieren. Die Organisation sollte einen angemessenen Entscheidungsfindungsprozess einschließlich entsprechender Politiken und Kontrollen festlegen und aufrechterhalten, welcher beinhaltet, dass die Entscheidungsträger über angemessene Befugnisse verfügen und frei von tatsächlichen oder potenziellen Interessenkonflikten sind.

Die oberste Leitung sollte sicherstellen, dass diese Prozesse als Teil ihrer Rolle und Verantwortlichkeit für die Umsetzung und Einhaltung des Hinweismanagementsystems regelmäßig überprüft werden.

6 Planung

6.1 Maßnahmen zum Umgang mit Risiken und Möglichkeiten

Bei Planungen für das Hinweismanagementsystem sollte die Organisation ihre bestehenden Politiken, Prozesse und Funktionen (Compliance, Recht, Berichterstattung, Beschaffung, Offenlegung, Kommunikation usw.), die in 4.1 genannten Themen und die in 4.2 genannten Anforderungen berücksichtigen sowie die Risiken und Chancen bestimmen, die betrachtet werden müssen, um

- sicherzustellen, dass das Hinweismanagementsystem seine beabsichtigten Ergebnisse erzielen kann;
 - die Meldung von Fehlverhalten zu fördern und zu erleichtern;
 - Hinweisgeber und andere beteiligte Personen zu unterstützen und zu schützen;
 - sicherzustellen, dass Berichten über Fehlverhalten ordnungsgemäß und zeitnah nachgegangen wird;
 - Organisationskultur, Governance und vorbeugende Maßnahmen gegen Fehlverhalten zu verbessern.
- unerwünschte Auswirkungen zu verhindern oder zu verringern; und
- fortlaufende Verbesserung zu erreichen.

Die Organisation sollte planen:

- a) Maßnahmen zum Umgang mit diesen Risiken und Chancen;
- b) wie:
 - die Maßnahmen in die Prozesse des Hinweismanagementsystems der Organisation integriert und dort umgesetzt werden;
 - die Wirksamkeit dieser Maßnahmen bewertet wird;
 - relevantes Personal und relevante interessierte Parteien in die Planung des Hinweismanagementsystems einbezogen werden;
 - Vorkommnisse zu behandeln sind, in denen Fehlverhalten außerhalb der Organisation gemeldet werden (z. B. den zuständigen Behörden);
 - hoch das Ausmaß der Vertraulichkeit, der Unterstützung und des Schutzes ist, das die Organisation im Rahmen des Hinweismanagementsystems bieten kann, sowie
 - Rückmeldung zu geben sowie vom Hinweisgeber und anderen relevanten interessierten Parteien einzuholen ist.

6.2 Ziele des Hinweismanagementsystems und Planung zu deren Erreichung

Die Organisation sollte ihre Ziele des Hinweismanagementsystems für relevante Funktionen und Ebenen festlegen.

Die Ziele des Hinweismanagementsystems sollten:

- a) im Einklang mit der Politik zu Hinweisgebermeldungen stehen;
- b) messbar sein (sofern machbar);

- c) anwendbare Anforderungen berücksichtigen;
- d) überwacht werden;
- e) bewertet werden;
- f) vermittelt werden;
- g) soweit erforderlich, aktualisiert und/oder überarbeitet werden sowie
- h) sicherstellen, dass das Hinweismanagementsystem die frühzeitige Entdeckung und Verhinderung von Fehlverhalten erleichtern kann.

Die Organisation sollte dokumentierte Informationen zu den Zielen des Hinweismanagementsystems aufbewahren.

Bei der Planung zum Erreichen der Ziele des Hinweismanagementsystems sollte die Organisation bestimmen:

- was getan wird;
- welche Ressourcen erforderlich sind;
- wer verantwortlich ist;
- wann es abgeschlossen wird;
- wie die Ergebnisse überwacht und bewertet werden;
- wie sie ggf. aktualisiert werden und
- wie die Ergebnisse vermittelt werden.

7 Unterstützung für das Hinweismanagementsystem

7.1 Ressourcen

Die Organisation sollte die erforderlichen Ressourcen für den Aufbau, die Entwicklung, die Verwirklichung, die Beurteilung, die Aufrechterhaltung und die fortlaufende Verbesserung des Hinweismanagementsystems und zur Erreichung ihrer Ziele bestimmen und bereitstellen.

Die Ressourcen können unter anderem die finanziellen und personellen Ressourcen, IT-Lösungen, Fachkenntnisse, Organisationsinfrastruktur, Untersuchungspersonen, aktuelle Referenzmaterialien zu Hinweisgebermeldungen, rechtliche Fachkenntnisse sowie berufliche Weiterbildung und Schulung umfassen. Diese Ressourcen können intern oder extern zur Verfügung gestellt werden.

ANMERKUNG Je nach Größe, Komplexität, Struktur, Betriebsabläufen und anderen Überlegungen, auf die in 4.1, 4.2 und 4.3 Bezug genommen wird, können Organisationen bestimmte Funktionen des Hinweismanagementsystems ausgliedern. Organisationen können die Erfassung, Verarbeitung und Untersuchung von Fehlverhalten an unabhängige Dritte oder externe Dienstleister wie Lösungsanbieter für Hinweismanagementsysteme, Beratungsdienstleister, Ombudspersonen usw. ausgliedern.

7.2 Kompetenz

Die Organisation sollte:

- für jedwede Personen, die unter ihrer Aufsicht Tätigkeiten verrichten, welche das Hinweismanagementsystem der Organisation sowie dessen Leistung und Betrieb beeinflussen, die erforderliche Kompetenz bestimmen;
- sicherstellen, dass jedwede Personen, die in das Hinweismanagementsystem einbezogen sind, auf Grundlage angemessener Ausbildung, Schulung oder Erfahrung kompetent sind;
- sicherstellen, dass, sofern relevant, das Personal in der Lage ist, mit der angemessenen Unparteilichkeit tätig zu sein;
- wenn erforderlich, Maßnahmen einleiten, um die benötigte Kompetenz zu erwerben, und die Wirksamkeit der getroffenen Maßnahmen zu bewerten;
- angemessene dokumentierte Information als Nachweis der Kompetenz aufbewahren;
- sicherstellen, dass die Hinweismanagementfunktion über einen direkten, ungehinderten Zugang zu ausreichenden Ressourcen (siehe 7.1) verfügt, um Unparteilichkeit, Nachverfolgbarkeit und Transparenz des Hinweismanagementsystems und seiner Prozesse sicherzustellen, sowie
- sicherstellen, dass die Hinweismanagementfunktion über einen direkten, unbeschränkten und vertraulichen Zugang zur obersten Leitung und zum obersten Organ verfügt.

Die Verantwortlichen für die Durchführung von Tätigkeiten im Zusammenhang mit Schutz und Untersuchung sollten unter anderem die folgenden Eigenschaften aufweisen:

- Vertrauenswürdigkeit;
- emotionale Intelligenz;
- diplomatisches Geschick;
- Unparteilichkeit;
- Integrität;
- Führungsstärke;
- Vertraulichkeit;
- sicheres Urteilsvermögen;

ANMERKUNG Geeignete Maßnahmen können zum Beispiel sein: Schulung, Mentoring oder Versetzung von Personal, oder Anstellung oder Beauftragung kompetenter Personen.

7.3 Bewusstsein und Schulung

7.3.1 Allgemeines

Personen, die unter Aufsicht der Organisation Tätigkeiten verrichten, sollten sich:

- der Politik zu Hinweisgebermeldungen (siehe 5.2);
- der Ziele des Hinweismanagementsystems (siehe 6.2);
- ihres Beitrags zur Wirksamkeit des Hinweismanagementsystems, einschließlich der Vorteile einer verbesserten Leistung des Hinweismanagementsystems (siehe 10.2) und