DIN ISO 37002

DIN

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

Bilder

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 beigefügt. 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-

mentsysteme 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.

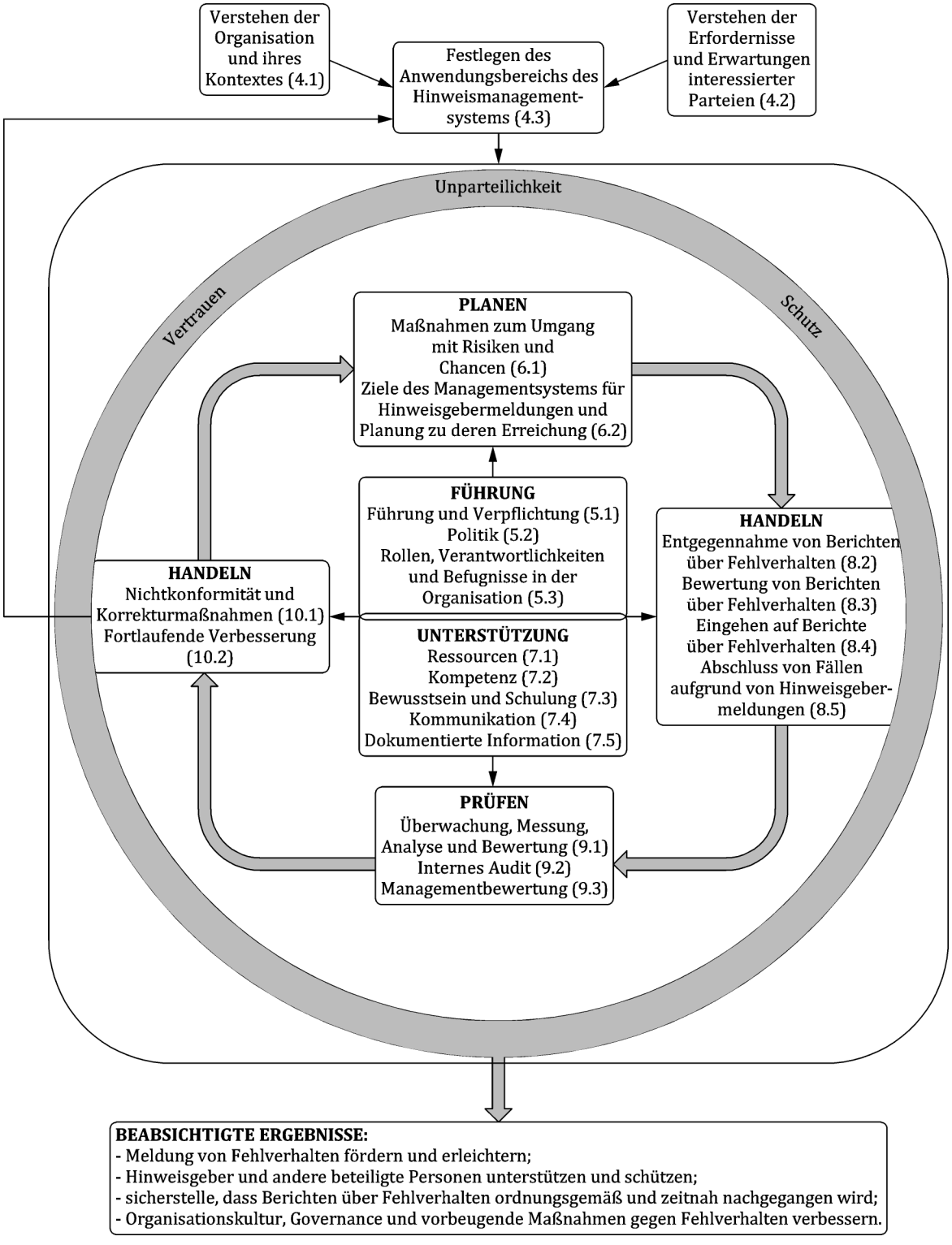

Bild 1 — Übersicht eines Hinweismanagementsystems