— Ergebnisse von Audits sowie Überwachungsaktivitäten.

Die Compliance-Politik sollte die unmittelbare Meldung von Angelegenheiten, die außerhalb der regulären Berichtszeiten auftreten, unterstützen.

A.9.1.5 Aufzeichnungen

Aufzeichnungen sollten die Aufzeichnung und Klassifizierung von Compliance-Problemen und angeblichen Non-Compliance-Fällen sowie die zu ihrer Lösung unternommenen Schritte enthalten.

Aufzeichnungen sollten so gespeichert werden, dass sie dauerhaft lesbar, direkt identifizierbar und abrufbar bleiben.

Diese Aufzeichnungen sollten vor Hinzufügung, Löschung, Veränderung, unbefugter Nutzung oder Verschleierung geschützt sein.

Die Aufzeichnungen des Compliance-Managementsystems der Organisation können Folgendes beinhalten:

— Informationen über die Compliance-Leistung, einschließlich Compliance-Berichte;

— Einzelheiten zu Non-Compliance und Korrekturmaßnahmen;

— Ergebnisse der Überprüfungen und Audits des Compliance-Managementsystems und der getroffenen Maßnahmen.

A.9.2 Internes Audit

Interne und externe Auditfunktionen müssen frei von Interessenkonflikten und unabhängig sein, um ihre Rolle zu erfüllen.

Sieh ISO 19011:2018 für Informationen zur Durchführung einer Audit eines Managementsystems.

A.9.3 Managementprüfung

Die Managementprüfung sollte außerdem Empfehlungen enthalten zu:

— erforderlichen Änderungen der Compliance-Politik, ihrer Ziele, Systeme, Struktur und ihres Personals;

— Änderungen der Compliance-Prozesse, um eine wirksame Integration in Betriebspraktiken und Systeme sicherzustellen;

— auf potenzielle zukünftige Non-Compliance zu überwachende Bereiche;

— Korrekturmaßnahmen in Bezug auf Non-Compliance;

— Lücken oder Mängel der aktuellen Compliance-Systeme und längerfristige ständige Verbesserungsinitiativen;

— Anerkennung vorbildhaften Compliance-Verhaltens innerhalb der Organisation.

Eine Kopie der dokumentierten Ergebnisse und aller Empfehlungen der Managementprüfung sollte dem obersten Organ übermittelt werden.

A.10 Verbesserung

A.10.1 Nichtkonformität und Korrekturmaßnahmen

Das Versäumnis, einmalige Non-Compliance-Fälle zu verhindern oder zu erkennen, bedeutet nicht notwendigerweise, dass das Compliance-Managementsystem nicht grundsätzlich wirksam Non-Compliance verhindert und erkennt.

Informationen aus der Analyse von Nichtkonformität oder Non-Compliance kann verwendet werden, um Folgendes zu berücksichtigen:

— Beurteilung der Leistung von Produkten und Dienstleistungen;

— Verbesserung und/oder Umgestaltung von Produkten und Dienstleistungen;

— Änderung von Praktiken und Verfahren der Organisation;

— Nachschulung von Mitarbeitern;

— Beurteilung der Notwendigkeit, interessierte Parteien zu informieren;

— Bereitstellung frühzeitiger Warnung vor potenzieller Non-Compliance;

— Umgestaltung oder Überprüfung von Kontrollen;

— Verbesserung von Benachrichtigungs- und Weiterleitungsschritten (intern und extern);

— Kommunikation von Fakten zur Non-Compliance und der Position der Organisation hinsichtlich der Non-Compliance.

A.10.2 Ständige Verbesserung

Die Wirksamkeit eines CMS wird durch die Tatsache charakterisiert, dass es kontinuierlich verbessert und weiterentwickelt werden kann. Die interne und externe Umgebung der Organisation und das Geschäft verändern sich im Lauf der Zeit ebenso wie die Eigenschaften ihrer Kunden und gegebenenfalls der Compliance-Verpflichtungen.

Die Eignung und Wirksamkeit des Compliance-Managementsystems sollte kontinuierlich und regelmäßig durch verschiedene Verfahren wie etwa Prüfungen durch interne Audits beurteilt werden.

Die Organisation sollte Maßnahmen zur Prüfung ihres CMS erstellen und sicherstellen, dass diese aktuell und für den Zweck geeignet bleiben. Die Organisation sollte bei der Bestimmung des Umfangs und Zeitrahmens von Maßnahmen zur Unterstützung der ständigen Verbesserung ihren Kontext, wirtschaftliche Faktoren und andere relevante Umstände berücksichtigen.

Einige Organisationen befragen ihre Mitarbeiter, um die Compliance-Kultur zu messen und die Stärke der Kontrollen zu bewerten. Weitere Informationsquellen für die ständige Verbesserung können Ergebnisse von Kundenumfragen, Berichte zu gemeldeten Bedenken, regelmäßige Überwachung, regelmäßige Audits oder Managementprüfungen sein.

Die Organisation sollte anhand der Ergebnisse dieser Bewertungen bestimmen, ob es einen Bedarf oder eine Gelegenheit zum Ändern des Compliance-Managementsystems gibt.

Um die Integrität des Compliance-Managementsystems und seine Wirksamkeit zu gewährleisten, sollten Änderungen in einzelnen Elementen des Managementsystems die Abhängigkeit und die Auswirkungen solcher Änderungen auf die Wirksamkeit des Managementsystems als Ganzes berücksichtigen.

Wenn Änderungen an dem CMS vorgenommen werden, sollte die Organisation die Implikationen dieser Änderungen für das CMS, seinen Betrieb, die Verfügbarkeit von Ressourcen, die Compliance-Risikobeurteilungen, die Compliance-Verpflichtungen der Organisation und ihre ständigen Verbesserungsprozesse berücksichtigen.

Literaturhinweise

[1] ISO 9001, *Quality management systems — Requirements*

[2] ISO 10002, *Quality management — Customer satisfaction — Guidelines for complaints handling in organizations*

[3] ISO 14001, *Environmental management systems — Requirements with guidance for use*

[4] ISO 19011, *Guidelines for auditing management systems*

[5] ISO 22000, *Food safety management systems — Requirements for any organization in the food chain*

[6] ISO 26000, *Guidance on social responsibility*

[7] ISO 31000, *Risk management — Guidelines*

[8] ISO 37001, *Anti-bribery management systems — Requirements with guidance for use*

[9] ISO Guide 73, *Risk management — Vocabulary*

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 309 *Governance of organizations*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

This document cancels and replaces ISO 19600:2014-10.

In this International Standard, the following verbal forms are used:

— "shall" indicates a requirement;

— "should" indicates a recommendation;

— "may" indicates permission:

— "can" indicates a possibility or a capability.

Information marked as "NOTE" is for guidance in understanding or clarifying the associated requirements.

Introduction

Organizations that aim to be successful in the long term need to establish and maintain a culture of integrity and compliance, considering the needs and expectations of interested parties. Integrity and compliance are therefore not only the basis, but also an opportunity, for a successful and sustainable organization.

Compliance is an ongoing process and the outcome of an organization meeting its obligations. Compliance is made sustainable by embedding it in the culture of the organization and in the behaviour and attitude of people working for it. While maintaining its independence, it is preferable if compliance management is integrated with the organization's other management processes and its operational requirements and procedures.

An effective, organization-wide compliance management system enables an organization to demonstrate its commitment to comply with relevant laws, including legislative requirements, industry codes and organizational standards, as well as standards of good corporate governance, best practices, ethics and community expectations.

An organization's approach to compliance is shaped by the leadership applying core values and generally accepted corporate governance, ethical and community standards. Embedding compliance in the behaviour of the people working for an organization depends above all on leadership at all levels and clear values of an organization, as well as an acknowledgement and implementation of measures to promote compliant behaviour. If this is not the case at all levels of an organization, there is a risk of noncompliance.

In a number of jurisdictions, courts have considered an organization's commitment to compliance through its compliance management system when determining the appropriate penalty to be imposed for contraventions of relevant laws. Therefore, regulatory and judicial bodies can also benefit from this document as a benchmark.

Organizations are increasingly convinced that by applying binding values and appropriate compliance management, they can safeguard their integrity and avoid or minimize noncompliance with the organization's compliance obligations. Integrity and effective compliance are therefore key elements of good and diligent management. Compliance also contributes to the socially responsible behaviour of organizations.

One of the objectives of this document is to assist organizations to develop and spread a positive culture of compliance, considering that an effective and sound management of compliance-related risks should be regarded as an opportunity to pursue and take, due to the several benefits that it provides to the organization.

This document specifies requirements as well as provides guidance on compliance management systems and recommended practices. Both the requirements and the guidance in this document are intended to be adaptable, and the implementation of this can differ depending on the size and level of maturity of an organization's compliance management system and on the context, nature and complexity of the organization's activities and objectives.

This document is suitable to enhance the compliance-related requirements in other management systems and to assist an organization in improving the overall management of all its compliance obligations.

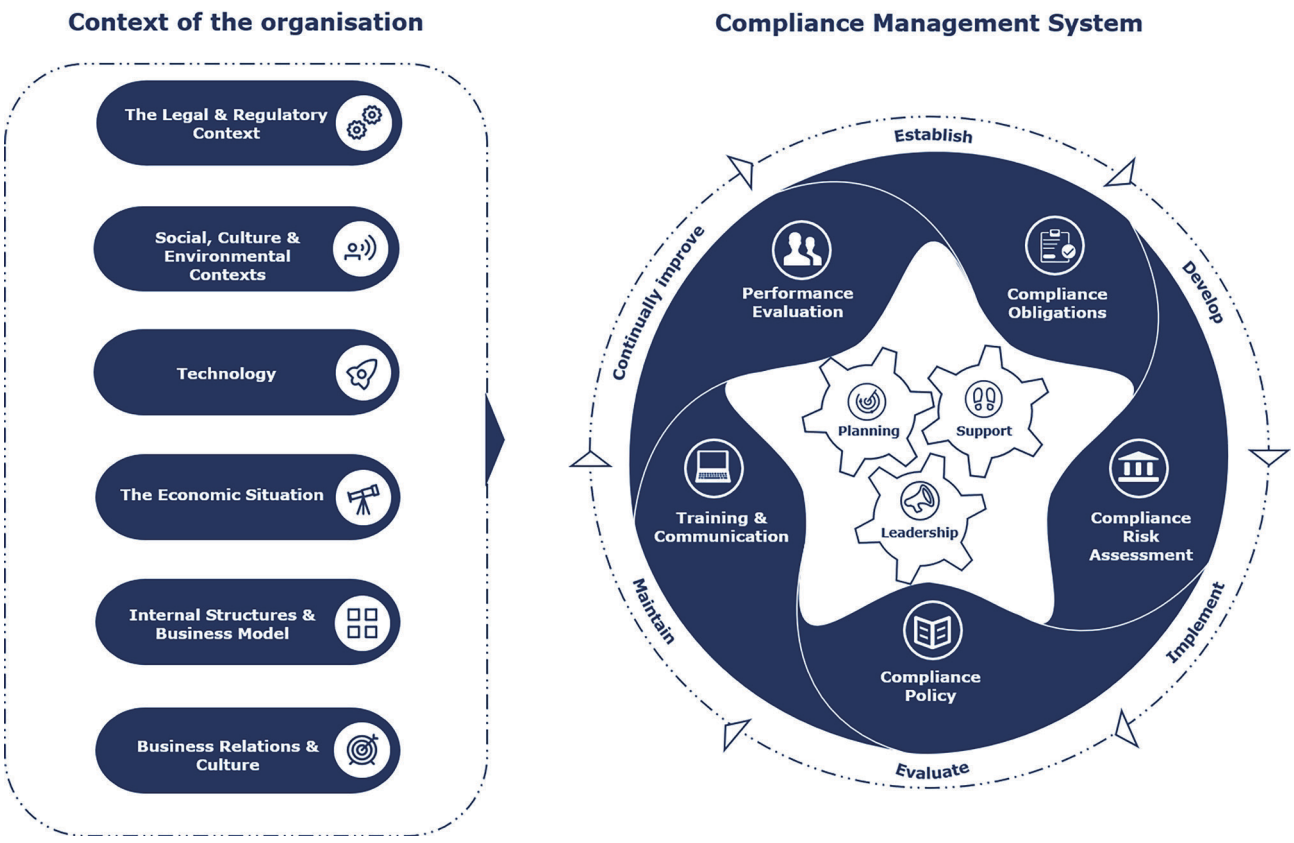

Figure 1 —