ČESKÁ TECHNICKÁ NORMA

ICS 03.100.01; 03.100.02; 03.100.70 **Červenec 2023**

Systémy managementu souladu – Požadavky s návodem pro použití

ČSN ISO 37301

01 0394

Compliance management systems – Requirements with guidance for use

Systemes de management de la conformité – Exigences et recommandations pour la mise en oeuvre

Tato norma je českou verzí mezinárodní normy ISO 37301:2021. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO 37301:2021. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO 37301 (01 0394) z října 2021.

Národní předmluva

Souvisící ČSN a TNI

ČSN EN ISO 9000 (01 0300) Systémy managementu kvality – Základní principy a slovník

ČSN EN ISO 9001 (01 0321) Systémy managementu kvality – Požadavky

ČSN EN ISO 14001 (01 0901) Systémy environmentálního managementu – Požadavky s návodem pro použití

ČSN EN ISO 19011 (01 0330) Směrnice pro auditování systémů managementu

ČSN EN ISO 22000 (56 9600) Systémy managementu bezpečnosti potravin – Požadavky na organizaci v potravinovém řetězci

ČSN EN ISO 26000 (01 0390) Pokyny pro oblast společenské odpovědnosti

ČSN EN ISO/IEC 27001 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky

ČSN ISO 31000 (01 0351) Management rizik – Směrnice

ČSN EN IEC 31010 ed. 2 (01 0352) Management rizik – Techniky posuzování rizik

ČSN ISO 37001 (01 0392) Systémy protikorupčního managementu – Požadavky s návodem pro použití

ČSN ISO 37002 (01 0395) Systémy managementu oznamování protiprávního jednání – Směrnice

TNI 01 0350 (01 0350) Management rizik – Slovník (Pokyn 73)

Vypracování normy

Zpracovatel: Mgr. Jakub Neumann, IČO 49853368

Technická normalizační komise: TNK 6 Management kvality a prokazování kvality

Pracovník České agentury pro standardizaci: Ing. Radmila Foretová

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

MEZINÁRODNÍ NORMA

Systémy managementu souladu – Požadavky s návodem pro použití

ISO 37301

První vydání
2021-04

ICS 03.100.01; 03.100.02; 03.100.70

Obsah

Contents

DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO 2021
Veškerá práva vyhrazena. Žádná část této publikace nesmí být, není-li specifikováno jinak nebo nepožaduje-li se to v souvislosti s její implementací, reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým ani mechanickým, včetně pořizování fotokopií nebo zveřejňování na internetu nebo intranetu, bez předchozího písemného souhlasu. O souhlas lze požádat buď ISO na níže uvedené adrese, nebo členskou organizaci ISO v zemi žadatele.
ISO copyright office
CP 401 · Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Tel.: + 41 22 749 01 11
E-mail: copyright@iso.org
Web: www.iso.org
Publikováno ve Švýcarsku

Předmluva

ISO (Mezinárodni´ organizace pro normalizaci) je celosvětová federace národních normalizačních orgánů (členů ISO). Mezinárodní normy obvykle vypracovávají technické komise ISO. Každý´ člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být v této technické komisi zastoupen. Práce se zúčastňují také vládní i nevládní mezinárodni´ orga-
nizace, s nimižˇ ISO navázala pracovní styk. ISO úzce spolupracuje s Mezinárodni´ elektrotechnickou komisi´ (IEC) ve všech záležitostech normalizace v elektro-technice.

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.

Postupy použité při tvorbě tohoto dokumentu a postupy určené pro jeho další udržováni´ jsou popsány ve směrnicích ISO/IEC, část 1. Zejména se má věnovat pozornost rozdílným schvalovacím kritériím potřebným pro různé druhy dokumentu° ISO. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnicích ISO/IEC, část 2 (viz www.iso.org/directives).
Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO nelze činit odpovědnou za identifikaci jakéhokoliv nebo všech patentových práv. Podrobnosti o jakýchkoliv patentových právech identifikovaných během přípravy tohoto dokumentu budou uvedeny v úvodu a/nebo v seznamu patentových prohlášeni´ obdržených ISO (viz www.iso.org/patents).
Jakýkoliv obchodní název použity´ v tomto dokumentu se uvádí jako informace pro usnadněni´ práce uživatelů a neznamená schváleni´.
Vysvětlení nezávazného charakteru technických norem, významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy Světové obchodní organizace (WTO) týkající se technických překážek obchodu (TBT), jsou uvedeny na tomto odkazu URL:
www.iso.org/iso/foreword.html
Tento dokument vypracovala technická komise IS0/TC 309 S*práva a řízení organizací*.

Toto první vydání ISO 37301 zrušuje a nahrazuje ISO 19600:2014, která byla technicky revidována.
Hlavní změny proti ISO 19600:2014 jsou tyto:

– tento dokument nyní obsahuje požadavky s dodatečným návodem pro použití založeným na těchto požadavcích;
– tento dokument se řídí požadavky ISO na harmonizovanou strukturu norem systému managementu.
Jakákoli zpětná vazba nebo otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na adrese www.iso.org/members.html.

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 on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee IS0/TC 309, *Governance of organizations*.
This first edition of ISO 37301 cancels and replaces ISO 19600:2014, which has been technically revised.
The main changes compared to ISO 19600:2014 are as follows:
– this document now contains requirements with additional guidance for use based on those requirements;
– this document follows ISO,s requirements for a harmonized structure for management system standards.
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

Úvod

Organizace, které si kladou za cíl být dlouhodobě úspěšné, potřebují vytvořit a udržovat kulturu souladu s ohledem na potřeby a očekávání zainteresovaných stran. Soulad je tedy nejen základem, ale i příležitostí pro úspěšnou a udržitelnou organizaci.

Dosahování souladu je trvalý proces a výstup organizace, která plní své povinnosti. Dosahování souladu se stává udržitelné tím, že je zakotveno v kultuře organizace a v chování a přístupu lidí, kteří pro ni pracují. Při zachování nezávislosti je žádoucí, aby management souladu byl integrován s ostatními řídicími procesy organizace a jejími provozními požadavky a postupy.

Efektivní systém managementu souladu v celé organizaci umožňuje organizaci prokázat svůj závazek dodržovat příslušné zákony, regulační požadavky, kodexy odvětví a organizační standardy, jakož i standardy řádné správy a řízení, obecně uznávané nejlepší praxe, etiku a očekávání společenství.

Přístup organizace k dosahování souladu je utvářen vedením, které uplatňuje základní hodnoty a obecně přijímané standardy řádné správy a řízení, etické a společenské normy. Zakotvení dosahování souladu v chování lidí pracujících pro organizaci závisí především na vedení na všech úrovních a jasných hodnotách organizace, jakož i na uznání a implementaci opatření na podporu chování v souladu s pravidly. Pokud tomu tak není na všech úrovních organizace, existuje riziko nesouladu.

V řadě jurisdikcí při určování přiměřené sankce za porušení příslušných zákonů přihlížejí soudy k závazku souladu prostřednictvím systému managementu souladu. Proto mohou regulační a soudní orgány rovněž využít tento dokument jako měřítko.

Introduction

Organizations that aim to be successful in the long term need to establish and maintain a culture of compliance, considering the needs and expectations of interested parties. Compliance is 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 that 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, regulatory requirements, industry codes and organizational standards, as well as standards of good governance, generally accepted best practices, ethics and community expectations.

An organization,s approach to compliance is shaped by the leadership applying core values and generally accepted good 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.

Organizace jsou stále více přesvědčeny, že uplatňováním závazných hodnot a vhodným managementem souladu mohou chránit svou integritu a zabránit nesouladu s povinnostmi organizace v oblasti dosahování souladu nebo jej minimalizovat. Integrita a efektivita souladu jsou proto klíčovými prvky správného a náležitého řízení. Dosahování souladu rovněž přispívá ke společensky odpovědnému chování organizací.

Jedním z cílů tohoto dokumentu je pomoci organizacím rozvíjet a šířit pozitivní kulturu souladu tím, že efektivní a řádné řízení rizik souvisejících se souladem má být považováno za příležitost, kterou je třeba sledovat a využít, a to vzhledem k několika přínosům, které organizaci přináší, jako jsou

– zlepšení obchodních příležitostí a udržitelnosti;
– ochrana a posílení pověsti a důvěryhodnosti organizace;
– zohlednění očekávání zainteresovaných stran;
– prokázání závazku organizace efektivně a účinně řídit svá rizika souladu;

– zvýšení důvěry třetích stran ve schopnost organizace dosáhnout udržitelného úspěchu;

– minimalizace rizika, že dojde k porušení a s tím spojeným nákladům a poškození dobrého jména.

Tento dokument specifikuje požadavky a také poskytuje návod pro systémy managementu souladu a doporučené praxe. Požadavky i návod uvedené v tomto dokumentu jsou určeny k přizpůsobení a implementace se může lišit v závislosti na velikosti a úrovni vyspělosti systému managementu souladu organizace a na kontextu, povaze a složitosti činností a cílů organizace.

Tento dokument je vhodný k rozšíření požadavků souvisejících s dosahováním souladu v jiných systémech managementu a k tomu, aby organizaci pomohl zlepšit celkové řízení všech jejích povinností v oblasti dosahování souladu.

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 such as:

– improving business opportunities and sustainability;
– protecting and enhancing an organization,s reputation and credibility;

– taking into account expectations of interested parties;
– demonstrating an organization,s commitment to managing its compliance risks effectively and efficiently;
– increasing the confidence of third parties in the organization,s capacity to achieve sustained success;
– minimizing the risk of a contravention occurring with the attendant costs and reputational damage.

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 implementation 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.

Obrázek 1 poskytuje přehled obecných prvků systému managementu souladu.

Figure 1 provides an overview on common elements of a compliance management system.

Obrázek 1 – Prvky systému managementu souladu

Figure 1 – Elements of a compliance management system

V tomto dokumentu se používají tyto slovesné tvary:
– „musí“ vyjadřuje požadavek;
– „má“ vyjadřuje doporučení;
– „smí“ vyjadřuje dovolení;
– „může“ vyjadřuje možnost nebo způsobilost.
Informace s označením „POZNÁMKA“ slouží jako návod pro pochopení nebo objasnění souvisejících požadavků.
Příloha A obsahuje návod pro použití tohoto dokumentu.

In this document, 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.
Annex A provides guidance for the use of this document.

1 Předmět normy

Tento dokument specifikuje požadavky a poskytuje směrnice pro vytvoření, vývoj, implementaci, hodnocení, udržování a zlepšování efektivního systému manage-mentu souladu v organizaci.

Tento dokument je použitelný pro všechny typy orga-nizací bez ohledu na typ, velikost a povahu činností, jakož i na to, zda se jedná o organizaci z veřejného, soukromého nebo neziskového sektoru.
Všechny požadavky specifikované v tomto dokumentu, které se odkazují na správní a řídicí orgán, se vztahují na vrcholové vedení v případě, kdy organizace nemá správní a řídicí orgán jako samostatnou funkci.

1 Scope

This document specifies requirements and provides guidelines for establishing, developing, implementing, evaluating, maintaining and improving an effective compliance management system within an organization.
This document is applicable to all types of organizations regardless of the type, size and nature of the activity, as well as whether the organization is from the public, private or non-profit sector.

All requirements specified in this document that refer to a governing body apply to top management in cases where an organization does not have a governing body as a separate function.

Konec náhledu - text dále pokračuje v placené verzi ČSN.