ICS 35.020 SLOVENSKÁ TECHNICKÁ NORMA Júl 2024

STN	**Informačné technológie** **Strategické vedenie IT pre organizáciu**	**STN** **ISO/IEC 38500** 97 4186

Information technology
Governance of IT for the organization

Technologies de l'information
Gouvernance des technologies de l'information pour l'entreprise

Informationstechnologie
IT-Governance der Organisation

Táto slovenská technická norma obsahuje anglickú verziu medzinárodnej normy ISO/IEC 38500: 2024 a má postavenie oficiálnej verzie.

This Slovak standard includes the English version of the International standard ISO/IEC 38500: 2024 and has the status of the official version.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza STN ISO/IEC 38500 z mája 2011 v celom rozsahu.

138736

Anotácia

Toto tretie vydanie ruší a nahrádza druhé vydanie (ISO/IEC 38500: 2015), ktoré bolo technicky revidované.

Hlavné zmeny sú nasledovné:

- boli vypracované zásady strategického vedenia IT a zosúladenie so zásadami riadenia v ISO 37000;
- model bol aktualizovaný tak, aby zahŕňal „zapojenie zainteresovaných strán“;
- rámec pre riadenie IT bol aktualizovaný z ISO/IEC TR 38502.

Tento dokument poskytuje hlavné zásady pre členov riadiacich orgánov organizácií a tých, ktorí ich podporujú pri účinnom, efektívnom a prijateľnom využívaní informačných technológií (IT) v rámci ich organizácií.

Tento dokument sa vzťahuje na:

- strategické vedenie súčasného a budúceho využívania IT v organizácii;
- strategické vedenie IT ako domény riadenia organizácií.

Pokiaľ ide o publikum, tento dokument sa vzťahuje na:

- všetky organizácie vrátane verejných a súkromných spoločností, vládnych subjektov a neziskových organizácií;
- organizácie všetkých veľkostí, od najmenších po najväčšie, bez ohľadu na rozsah ich využívania IT.

Národný predhovor

Normatívne referenčné dokumenty

Na nasledujúce dokumenty sa odkazuje v texte takým spôsobom, že časť ich obsahu alebo celý obsah predstavuje požiadavky tohto dokumentu. Pri datovaných odkazoch sa používa len citované vydanie. Pri nedatovaných odkazoch sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek zmien).

POZNÁMKA 1. – Ak bola medzinárodná publikácia zmenená spoločnými modifikáciami, čo je indikované označením (mod), použije sa príslušná EN/HD.

POZNÁMKA 2. – Aktuálne informácie o platných a zrušených STN a TNI možno získať na webovom sídle www.unms.sk.

ISO 37000 prijatá ako STN ISO 37000 Spravovanie organizácií. Usmernenie (01 0109)

Vypracovanie slovenskej technickej normy

Spracovateľ: Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, Bratislava

Technická komisia: TK 37 Informačné technológie

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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 document 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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 40, *IT service management and IT governance*.

This third edition cancels and replaces the second edition (ISO/IEC 38500:2015), which has been technically revised.

The main changes are as follows:

— the principles for governance of IT and alignment to the principles of governance in ISO 37000 have been elaborated;

— the model has been updated to include "engage stakeholders";

— a framework for the governance of IT has been updated from ISO/IEC TR 38502.

A list of all parts in the ISO/IEC 38500 series can be found on the ISO and IEC websites.

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 and www.iec.ch/national-committees.

Introduction

The use of information technology (IT) is critical to the success of most organizations, not only as a supporting function, but also as part of the organization's capability to transform the organization. IT enables new business models and can substantially improve the organization's outcomes to meet the organization's stakeholder needs and expectations. The growing threat of cybersecurity and risks emanating from emerging technologies increases this focus.

The increasing potential of current and future IT requires the appropriate application of governance of IT to ensure that it fulfils the purpose of the organization in an effective, responsible and ethical manner, and that it aligns with the organization's strategic direction.

The objective of this document is to provide guidance to governing bodies on the responsible, innovative, sustainable and strategic use of IT, data and digital capabilities, so their organizations can fulfil their purpose in a manner expected by their stakeholders. This document provides principle-based guidelines and therefore does not include specific implementation detail.

It utilizes three tools for the governing body and associated governance and management practices to achieve good governance of IT:

1) Principles for the governance of IT — applying these principles to the responsible and strategic use of IT can lead to an organization that is more agile and adaptive.

2) Model for the governance of IT — the model shows the main governance tasks and interactions throughout the organization, leading to a clarity of decision-making and responsibilities for all aspects of the use of IT.

3) Framework for the governance of IT — the framework describes the elements through which the organization's governance of IT arrangements operate, which helps to ensure the critical actions of governance are considered and applied to the use of IT by the organization.

As the governance of IT is a domain of the governance of organizations, this document aligns to ISO 37000 and its principles of governance. This document can also be used in conjunction with other governance codes and principles for effective governance. This document can be used independently or to upgrade current governance based on the previous edition of ISO/IEC 38500.

This document is addressed primarily to the governing body but recognizes that governance occurs throughout the organization. It therefore provides guidance on the practice of governance of IT across the organization including the interaction and collaboration of all personnel, regardless of their job description.

International Standard **ISO/IEC 38500:2024(en)**

Information technology — Governance of IT for the organization

1 Scope

This document provides guiding principles for members of governing bodies of organizations and those that support them on the effective, efficient and acceptable use of information technology (IT) within their organizations.

This document is applicable to:

— the governance of the organization's current, and future, use of IT;

— the governance of IT as a domain of governance of organizations.

In terms of audience, this document is applicable to:

— all organizations, including public and private companies, government entities, and not-for-profit organizations;

— organizations of all sizes, from the smallest to the largest, regardless of the extent of their use of IT.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 37000, *Governance of organizations — Guidance*