

2020

Informační technologie –
Správa a řízení IT technologií v organizaci

ČSN
ISO/IEC 38500

36 9045

Information technology – Governance of IT for the organization

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

Tato norma je českou verzí mezinárodní normy ISO/IEC 38500:2015. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 38500:2015. It was translated by the Czech Agency for Standardization. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

V tomto dokumentu nejsou žádné citované dokumenty.

Vysvětlivky k textu převzaté normy

Pro účely této normy byl použit:

- překlad anglického termínu „accountability“ jako „(prokazatelná) odpovědnost“ s ohledem na jeho preferované používání v oblasti IT a v návaznosti na vydané normy z oblasti IT, zejména normy řady 27000;
- překlad anglického termínu „responsibility“ jako „odpovědnost“ s ohledem na význam v textu normy.

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČO 40654419

Technická normalizační komise: TNK 20 Informační technologie

Pracovník České agentury pro standardizaci: Ing. Miroslav Škop

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.

ICS 35.080

Obsah

	Strana
Předmluva.....	
..... 4	
Úvod.....	
..... 5	
1..... Předmět	
normy.....	
..... 6	
2..... Termíny	
a definice.....	
..... 6	
3..... Výhody řádné správy a řízení	
IT.....	9
4..... Zásady a model pro řádnou správu a řízení	
IT.....	10
4.1.....	
Zásady.....	
..... 10	
4.2.....	
Model.....	
..... 10	
5..... Pokyny pro správu a řízení	
IT.....	12
5.1.....	
Obecně.....	
..... 12	
5.2..... Zásada 1:	
Odpovědnost.....	
..... 12	

5.3..... Zásada 2:	
Strategie.....	
.....	12
5.4..... Zásada 3:	
Akvizice.....	
.....	13
5.5..... Zásada 4:	
Výkonnost.....	
.....	13
5.6..... Zásada 5:	
Konformita.....	
.....	13
5.7..... Zásada 6: Lidské	
chování.....	
.....	14
Bibliografie.....	
.....	15



DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2015

Veškerá práva vyhrazena. Není-li specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým ani mechanickým, včetně pořizování fotokopii nebo zveřejnění na internetu nebo intranetu, bez předchozího písemného svolení. O písemné svolení lze požádat buď přímo ISO na níže uvedené adrese, nebo členskou organizaci ISO v zemi žadatele.

ISO copyright office

Case postale 56 · CH 1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail copyright@iso.org

Web www.iso.org

Publikováno ve Švýcarsku

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezi-národních norem prostřednictvím svých technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oborech společného zájmu. Práce se zúčastňují také další vládní i nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

Postupy použité při tvorbě tohoto dokumentu a postupy určené pro jeho další udržování jsou popsány ve směrnících ISO/IEC, část 1. Zejména se má věnovat pozornost rozdílným schvalovacím kritériím potřebným pro různé druhy dokumentů. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnících ISO/IEC, část 2 (viz www.iso.org/directives).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými 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 prohlášení obdrženy ISO (viz www.iso.org/patents).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamena schválení.

Vysvětlení významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy WTO týkající se technických překážek obchodu (TBT), jsou uvedeny na tomto odkazu URL: [Foreword – Supplementary information](#).

ISO/IEC 38500 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*, SC 40 *Management IT služeb a správa IT*.

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 38500:2008), jehož kapitoly, články a obrázky byly technicky zrevidovány.

Úvod

Cílem této mezinárodní normy je poskytnout orgánům správy a řízení zásady, definice a model, použitelné při hodnocení, řízení a monitorování používání informačních technologií (IT) v jejich organizacích.

Tato mezinárodní norma představuje obecnou poradenskou normu založenou na zásadách. Kromě poskytování obecných pokynů o úloze orgánu správy a řízení vybízí organizace k používání vhodných norem podporujících jejich správu a řízení IT.

Většina organizací používá IT jako základní podnikatelský nástroj a jen málo z nich může efektivně fungovat bez IT. IT je také významným faktorem v budoucích podnikatelských plánech mnoha organizací.

Výdaje na IT mohou představovat významnou část výdajů organizace na finanční a lidské zdroje. Návržnost těchto investic však často není plně realizována a nepříznivé účinky na organizace mohou být značné.

Hlavními důvody těchto negativních výsledků jsou důraz na technické, finanční a plánovací aspekty IT aktivit, spíše než důraz na celkový podnikatelský kontext používání IT.

Tato mezinárodní norma poskytuje zásady, definice a model pro řádnou správu a řízení IT, aby pomohla těm na nejvyšší úrovni organizací porozumět a plnit jejich zákonné, regulatorní a etické závazky v souvislosti s používáním IT jejich organizacemi.

Tento mezinárodní standard je v souladu s definicí správy a řízení společnosti, která byla zveřejněna jako Zpráva Výboru pro finanční aspekty správy a řízení společnosti (Cadburyho zpráva) v roce 1992. Cadburyho zpráva rovněž poskytla základní definici správy a řízení společnosti v Zásadách správy a řízení společnosti OECD v roce 1999 (revidováno v roce 2004). Správa a řízení se odlišují od managementu a pro zamezení záměny jsou tyto dva pojmy definovány v této mezinárodní normě a rozpracovány v ISO/IEC TR 38502.

Tato mezinárodní norma je určena především orgánu správy a řízení. V některých (obvykle menších) organizacích mohou být členy orgánu správy a řízení rovněž výkonní manažeři. Tato mezinárodní norma je použitelná pro všechny organizace, od nejmenších po největší, bez ohledu na účel, design a strukturu vlastnictví.

Implementace správy a řízení IT je zahrnuta v ISO/IEC TS 38501.

1 Předmět normy

Tato mezinárodní norma poskytuje základní zásady pro členy orgánů správy a řízení organizací (to může zahrnovat vlastníky, ředitele, partnery, výkonné manažery nebo podobné) pro efektivní, účinné a přijatelné využívání informačních technologií (IT) v jejich organizacích.

Poskytuje také pokyny těm, kteří orgánům správy a řízení poskytují poradenství, informační nebo asistenční služby. Zde jsou zahrnuti:

- výkonní manažeři;
- členové skupin monitorujících zdroje v rámci organizace;
- externí obchodní nebo techničtí specialisté, jako jsou právníci nebo účetní, maloobchodní nebo průmyslová sdružení nebo profesní organizace;
- interní a externí poskytovatelé služeb (včetně konzultantů);
- auditoři.

Tato mezinárodní norma se vztahuje na správu a řízení současného a budoucího používání IT v organizaci, včetně procesů managementu a rozhodnutí souvisejících se současným a budoucím používáním IT. Tyto procesy mohou být řízeny IT specialisty v rámci organizace, externími poskytovateli služeb nebo obchodními jednotkami v rámci organizace.

Tato mezinárodní norma definuje správu a řízení IT jako podskupinu nebo doménu správy a řízení organizace, nebo v případě společnosti jako podskupinu nebo doménu správy a řízení společnosti.

Tato mezinárodní norma je použitelná pro všechny organizace, včetně veřejných a soukromých společností, orgánů státní správy a neziskových organizací. Tato mezinárodní norma je použitelná pro organizace všech velikostí od nejmenších po největší, bez ohledu na rozsah jejich používání IT.

Účelem této mezinárodní normy je podpora efektivního, účinného a přijatelného používání IT ve všech organizacích cestou

- ujištění zúčastněných stran, že pokud budou dodržovány zásady a postupy navržené v normě, mohou mít důvěru ve správu a řízení IT organizace,
- informování a vedení orgánů správy a řízení při správě a řízení používání IT v jejich organizaci, a
- ustavení slovníku pro správu a řízení IT.

Konec náhledu - text dále pokračuje v placené verzi ČSN.