

Informační technologie –
Správa softwarových aktiv –
Část 1: Procesy a víceúrovňové posuzování shody

ČSN
ISO/IEC 19770-1
36 9043

Information technology – Software asset management –
Part 1: Processes and tiered assessment of conformance

Technologies de l'information – Gestion de biens de logiciel –
Partie 1: Procédés et évaluation progressive de la conformité

Tato norma je českou verzí mezinárodní normy ISO/IEC 19770-1:2012. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 19770-1:2012. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Souvisící ČSN

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

ČSN ISO/IEC 15504-2 (36 9027) Informační technologie – Posuzování procesu – Část 2: Realizace posouzení

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

Vypracování normy

Zpracovatel: Česká společnost pro jakost, z.s., IČ 00417955, Ing. Ondřej Hykš

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Miroslav Škop

MEZINÁRODNÍ NORMA

Informační technologie – Správa softwarových aktiv – ISO/IEC 19770-1
Část 1: Procesy a víceúrovňové posuzování shody Druhé vydání
2012-06-15

Obsah

Strana

Předmluva	5
Úvod	6
1 Předmět	8
1.1 Účel	8
1.2 Oblast použití	8
1.3 Omezení	9
2 Shoda	9
2.1 Zamýšlené užití	9
2.2 Způsoby prokazování plné shody	10
3 Termíny a definice	10
4 Procesy SAM	12
4.1 Obecně	12
4.2 Řídící prostředí SAM	14
4.3 Plánovací a implementační procesy SAM	18
4.4 Inventární procesy SAM	21
4.5 Procesy ověřování a zajišťování souladu SAM	24
4.6 Procesy provozního řízení a rozhraní pro SAM	27
4.7 Procesy a rozhraní životního cyklu SAM	31
5 Úrovně	36
5.1 Přehled	36
5.2 Úroveň 1 – důvěryhodná data	37
5.3 Úroveň 2 – procesy řízení organizace související se správou SAM	38
5.4 Úroveň 3 – hlavní procesy správy SAM	39
5.5 Úroveň 4 – úplná shoda SAM s ISO/IEC	40
Příloha A (informativní) Tabulka odkazů výstupů podle úrovně	41
Příloha B (informativní) Návod k vybraným tématům	46

[Příloha C \(informativní\) Vzájemné odkazy s návody na nejlepší postupy 47](#)

[Příloha D \(informativní\) Mapa 88](#)

[Příloha E \(informativní\) Přístupy způsobilosti/vyspělosti specifické pro odvětví 90](#)

[Bibliografie 94](#)



DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2012

Veškerá práva vyhrazena. Není-li specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně pořizování fotokopíí 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

Published in Switzerland

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 mezinárodních norem prostřednictvím svých technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují také další vládní a 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.

Návrhy mezinárodních norem jsou vypracovávány v souladu s pravidly danými směrnicemi ISO/IEC, část 2.

Hlavním úkolem společné technické komise je vypracování mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje schválení alespoň 75 % hlasujících národních orgánů.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikování jakéhokoli nebo všech patentových práv.

ISO/IEC 19770-1 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 7 *Softwarové a systémové inženýrství*.

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 19770-1:2006), které bylo technicky

zrevidováno.

ISO/IEC 19770 s společným názvem *Informační technologie – Správa softwarových aktiv* se sestává z těchto samostatných částí:

- Část 1: *Procesy a víceúrovňové posuzování shody*
- Část 2: *Identifikační značky softwaru*

Následující části se připravují:

- Část 3: *Označení oprávnění k softwaru*
- Část 5: *Přehled a slovník*

Část 5 bude stanovovat společný soubor terminologie pro řadu norem ISO/IEC 19770, který může aktualizovat definice uvedené v dříve vydaných částech.

Správa označení bude předmětem v budoucnu vytvořené části 7.

Úvod

Tato část ISO/IEC 19770 je určena organizacím, které chtějí dosáhnout nejlepších řešení ve správě softwarových aktiv (SAM). Vznikla na základě ISO/IEC 19770-1:2006 *Procesy správy softwarových aktiv*, která byla komplexní normou navrženou tak, aby byla v souladu s managementem služeb specifikovaným v ISO/IEC 20000.

Zpětná vazba z trhu ukázala, že organizace chtějí něco, co by bylo realizovatelné v několika úrovních, a to do té úrovně, která nejvíce vyhovuje potřebám organizace. Tato část ISO/IEC 19770 byla navržena tak, aby byli implementace SAM a soulad s vydanými normami realizovatelné v jakékoli z těchto úrovní. Tyto úrovně na sebe navazují. To umožňuje samostatnou, nezávislou certifikaci v souladu s přirozenými úrovněmi vývoje a prioritami správy SAM. Uznání souladu se uděluje organizacím na základě schopnosti veřejně prokazovat, že bylo dosaženo certifikace podle stanovené úrovně.

Rozdělení do úrovní je navrženo tak, aby většina organizací dokázala vytvořit standardizovaný SAM. Organizace, které implementují SAM poprvé, ho mohou často implementovat rychleji, pokud pečlivě stanoví rozsah zahrnutých softwarových aktiv a rozsah pokrytých částí organizace. Organizace běžně nepokrývají rozsahem všechny možné oblasti a rozsah softwaru a rozsah organizační struktury směřjí být určeny tak, jak je popsáno v kapitole 1 Předmět. Rozsah smí být stanoven jakýmkoli způsobem, ale musí být stanoven jednoznačně.

Pokud se organizace rozhodne tímto způsobem rozsah zúžit, měla by vzít v úvahu některé faktory, aby nedošlo k narušení schopnosti realizovat zamýšlené přínosy a dosáhnout cílů organizace. Například pro dobré zabezpečení je obvykle nezbytné, aby byla do rozsahu SAM zařazena všechna aktiva dotčených částí infrastruktury organizace. Navíc není možné spravovat softwarová aktiva bez souběžného spravování hardwaru, na kterém software funguje. Tuto část ISO/IEC 19770 je možné použít pro softwarová i hardwarová aktiva. Pojem SAM by měl pokrývat všechna aktiva týkající se softwaru, použití pojmu SAM v této části ISO/IEC 19770 navíc odráží organizační zařazení

odpovědné pracovní skupiny ISO/IEC a jeho používání v tržním prostředí. SAM má široké přínosy pro další související postupy správy IT aktiv a implementace správných postupů SAM, a může přinést další výhody nad rámec samotné správy softwaru.

Čtyři úrovně SAM definované touto částí ISO/IEC 19770 jsou zobrazeny na obrázku 1. Podrobnější popis čtyř úrovní viz kapitolu 5 Úrovně. Stručně mohou být popsány následujícím způsobem:



Obrázek 1 – Čtyři úrovně SAM

Hlavní přínosy spojené s jednotlivými úrovněmi jsou:

- Úroveň 1: Důvěryhodná data. Dosažení této úrovně znamená znalost aktiv, aby je bylo možné spravovat.

Ověřená data jsou základním předpokladem úspěšné správy SAM. I zde platí obecné pravidlo, že „nezle spravovat to, co není známo“. Tato úroveň představuje základ pro prokazování shody s licencí, který má vysokou strategickou prioritu.

POZNÁMKA Další části ISO/IEC 19770 stanovují Identifikační značky softwaru (ISO/IEC 19770-2 Software Identification Tag) a Označení oprávnění k softwaru (ISO/IEC 19770-3 Software Entitlement Tag), které mají zjednodušit získávání důvěryhodných dat.

- Úroveň 2: Procesy řízení organizace související se správou SAM. Dosažení této úrovně znamená zlepšování nástrojů správy SAM a dosahování okamžitých přínosů.

V praxi začíná management typicky řešit problémy související se SAM až v okamžiku, kdy jsou v organizaci zjištěny problémy s nedostatkem důvěryhodných dat. Organizace si uvědomuje rozsah rizik, kterým čelí, stejně jako příležitosti k optimalizaci a snižování nákladů. Tato úroveň pokrývá základní správu řídicího prostředí pro SAM (viz 4.2 Řídicí prostředí SAM), včetně politik, rolí a odpovědností. Zahrnuje také stanovování cílů a realizaci tzv. „rychlých výher“, které vyplývají z důvěryhodných dat z Úrovně 1.

- Úroveň 3: Hlavní procesy správy SAM. Dosažení této úrovně znamená zlepšování efektivnosti a účinnosti.

Tato úroveň znamená integraci SAM, založeného na Úrovních 1 a 2, do provozních procesů (viz 4.6 Procesy provozního řízení a rozhraní pro SAM). Výsledkem je zvýšená efektivnost a účinnost.

POZNÁMKA Další části ISO/IEC 19770 stanovují Identifikační značky softwaru (ISO/IEC 19770-2 Software Identification Tag) a Označení oprávnění k softwaru (ISO/IEC 19770-3 Software Entitlement Tag), které mají zjednodušit snahy o integraci.

- Úroveň 4: Úplná shoda SAM s ISO/IEC. Dosažení této úrovně znamená vybudování nejvyšší úrovně strategie nastavení SAM.

Tato úroveň řeší pokročilejší a náročnější aspekty SAM, včetně jeho úplné integrace do

strategického plánování organizace.

První tři úrovně jsou stanoveny jako podmnožiny celkového souboru procesních okruhů a výsledků stanovených v této části ISO/IEC 19770. To znamená, že každý procesní okruh má jeden cíl SAM, jako například identifikaci softwarových aktiv, a obsahuje několik výstupů procesů, které mají dosažení těchto cílů podporovat. Tabulka znázorňující tuto strukturu je uvedena v příloze A.

Úrovně na sobě navzájem staví a Úroveň 4 představuje celkový soubor procesních okruhů a výstupů stanovených v této části ISO/IEC 19770. Je třeba poznamenat, že procesní okruhy stanovené v této části ISO/IEC 19770 se, oproti ISO/IEC 19770:2006, výrazně nezměnily, byla pouze doplněna drobná vyjasnění textu. Struktura skupin procesů obsahujících více výstupů také nebyla změněna. Shody může být nyní dosaženo s ohledem na jakoukoli specifickou úroveň. Přestože je možné každou úroveň certifikovat zvlášť, každá závisí na průběžném plnění i předchozích úrovních. Prakticky by to znamenalo, že organizace procházející certifikací podle vyšší úrovně by byla podrobena v rámci běžného přezkoumání certifikačním orgánem dohledu nad předchozí úrovní nebo úrovněmi a zároveň přezkoumání vyšší úrovně.

Podrobnější vysvětlení stupňů a jejich charakteru je uvedeno v kapitole 5.

Celkové přínosy SAM mohou zahrnovat:

- a. **Řízení rizika:** například zmírňování rizik přerušení nebo snížení kvality IT služeb; právní rizika;
- b. **Řízení nákladů:** snížení přímých nákladů na software a snížení nákladů na software, vč. souvisejících aktiv (popis souvisejících aktiv viz 1.2) a nákladů na nepřetržitou podporu a smlouvy;
- c. **Konkurenční výhodu:** lepší obchodní rozhodnutí a spokojenost na základě vždy dostupných důvěryhodných dat.

Typickým provozním požadavkem může být zaměřit se na prioritní oblasti, například na určité výrobce softwaru nebo někdy na specifikovanou skupinu organizačních jednotek. Výběr úrovní v kombinaci se stanovováním cílů umožňuje mnoha organizacím realizovat přínosy ze standardizace procesů SAM popsaných v kapitole 1 Předmět.

Principiálně bude také možné ke stanovení standardu, kterého může být v jednotlivých fázích dosaženo, využít přístup založený na získaných zkušenostech a dosažené úrovni odbornosti. Pokud má být ale nezávisle certifikován, je takový přístup v praxi mnohem složitější. Navzdory tomu je záměrem v budoucnu takový přístup vytvořit, a to po dokončení plánované revize prvního vydání ISO/IEC 15504. To umožní sblížení přístupů založených na této části ISO/IEC 19770 a dalších tržních metodikách založených na posuzování vyspělosti organizace.

1 Předmět

1.1 Účel

Tato část ISO/IEC 19770 vytváří základ integrovaného souboru procesů správy softwarových aktiv (SAM), který je rozdělen do čtyř samostatných úrovní umožňujících postupnou implementaci, posuzování a uznávání procesů SAM.

1.2 Oblast použití

Tato část ISO/IEC 19770 se týká procesů SAM a organizace ji mohou implementovat za účelem dosažení okamžitých přínosů. ISO/IEC 19770-2 poskytuje souvisící specifikaci pro Identifikační značky softwaru. Aby bylo dosaženo plného rozsahu přínosů, měla by být tato specifikace implementována výrobcí softwaru (interními i externími), a vývojáři nástrojů.

Tato část ISO/IEC 19770 je zamýšlena jako implementační norma pro organizace. Budoucí vydání mohou poskytnout rámec pro měření v souladu s ISO/IEC 15504-2:2003 nebo budoucí mezinárodní normou ISO/IEC 330031).

Tato část ISO/IEC 19770 je aplikovatelná na všechny organizace bez ohledu na velikost nebo odvětví. Pro účely prokazování shody smí být tato část ISO/IEC 19770 aplikována pouze na právní subjekty nebo jejich části. Smí být také aplikována na několik právních subjektů (např. mateřská organizace a dceřiné organizace nadnárodního subjektu), za předpokladu, že mezi nimi existuje právní vazba, která umožňuje jednomu subjektu řídit ostatní. Platí pouze tam, kde řídicí subjekt má kontrolu nad celým rozsahem plnění (jak je definován pro účely posuzování shody) a subjekt posuzující shodu toto vymezení předmětu akceptuje.

POZNÁMKA Vymezení rozsahu plnění je dokumentováno jako součást Podnikového řídicího procesu pro SAM (4.2.2).

Tato část ISO/IEC 19770 smí být aplikována na organizace, které své procesy SAM zajišťují prostřednictvím externích zdrojů. Odpovědnost za prokazování shody ale vždy zůstává na organizaci, která si tyto zdroje objednáva.

Tato část ISO/IEC 19770 může být aplikována na veškerý software a souvisící aktiva, bez ohledu na povahu softwaru. Souvisící aktiva jsou taková, která mají charakteristiky nezbytné pro využití nebo správu softwaru. Lze ji například aplikovat na spustitelný software (jako jsou aplikace, operační systémy a programové nástroje) i na nespustitelný software (jako jsou fonty, obrázky, audio nebo video nahrávky, šablony, slovníky, dokumenty a data). Lze ji aplikovat na všechna technologická prostředí a počítačové platformy (např. virtualizované softwarové aplikace, lokálně instalované aplikace, software jako služba; je stejně aplikovatelná na cloudová řešení i na starší výpočetní prostředí).

POZNÁMKA Stanovení rozsahu softwarových aktiv (typy softwaru, které jsou zahrnuty do rozsahu) je dokumentováno jako součást plánu SAM vytvořeného v procesu *Plánování SAM*. Smí být stanoven způsobem, který organizace považuje za vhodný. Může například zahrnovat veškerý software, veškerý programový software, veškerý software na specifických platformách nebo software specifického výrobce. Rozsah ale musí být jednoznačný. Viz také další vysvětlení v tomto článku a v tabulce 1.

S výjimkou požadavků 4.7.4 Proces vývoje softwaru není požadavkem této části ISO/IEC 19770, aby byla aplikována na vývoj softwaru ve smyslu vývoje a udržování kódu. Je záměrem, aby byla aplikovatelná na veškerý software v provozním prostředí a na předběžné činnosti, jako je konfigurace softwaru a vytváření a řízení produkčních sestavení verzí a releasů. Jasná hranice mezi tím, co je považováno za čistý vývoj (a je tedy mimo předmět této normy) a tím, co je považováno za provozní prostředí (a spadá do předmětu této normy), může být určena s využitím jednoznačných formálních prohlášení rozsahu organizace a softwaru.

POZNÁMKA Software využívaný k vývoji jiného softwaru je považován za součást provozního prostředí, software využívaný vývojáři softwaru musí být sám o sobě spravován.

Následující kategorie softwarových aktiv patří do předmětu této části ISO/IEC 19770:

- a. práva k používání softwaru, a to jejich plné vlastnictví (v případně interně vyvinutého softwaru) a licence (pro většinu externě pořízeného softwaru, komerčního i open-source);
- b. používaný software, což zahrnuje hodnotu duševního vlastnictví softwaru (včetně originálního softwaru dodaného výrobcí nebo vývojáři, sestavení verzí softwaru a nainstalovaného softwaru a jiným způsobem poskytovaného, používaného a spouštěného softwaru); a
- c. média, na nichž jsou uloženy kopie používaného softwaru.

POZNÁMKA Z hlediska finančního účetnictví se za aktiva považují především položky spadající do kategorie (a), a i jejich hodnota již mohla být zcela odepsána. Z účetního hlediska lze kategorii (b) považovat spíše za závazky (nikoli aktiva), jedná-li se o komerční software, který není řádně licencován. Tato část normy ISO/IEC 19770 však považuje kategorie (b) a (c) za skutečná aktiva, která je nutná spravovat stejně jako kategorii (a). Licence mají sice účetní hodnotu, avšak především používaný software by měl mít obchodní hodnotu a je nutné jej považovat za obchodní majetek.

Souvisící aktiva v rozsahu působnosti této normy jsou veškerá další aktiva s charakteristikami nezbytnými pro použití nebo správu softwarových aktiv spadajících do rozsahu plnění. Všechny charakteristiky těchto souvisejících aktiv, které nejsou nezbytné pro použití nebo správu softwaru, jsou mimo rozsah plnění. Tabulka 1 uvádí příklady.

Tabulka 1 – Použití ISO/IEC 19770-1 na nesoftwarová aktiva

<i>Typ aktiva</i>	<i>Použití</i>	<i>Příklad</i>
<i>Hardware</i>	Normativní pro hardwarová aktiva s charakteristikami nezbytnými pro použití nebo správu softwarových aktiv, které patří do předmětu SAM	Seznam vybavení, na kterém může být software uchovávan, spouštěn nebo jinak používán; počet procesorů a výpočetní výkon; informace, zda je daný hardware započítán pro účely hromadných licencí
	Neaplikovatelná na charakteristiky, které nejsou nezbytné pro použití nebo správu softwarových aktiv, které patří do předmětu SAM	Náklady na pořízení hardwaru a jeho odpisy, plánování termínů pro včasné provedení obnovy softwarové podpory
<i>Další aktiva</i>	Normativní pro další aktiva s charakteristikami nezbytnými pro použití nebo správu softwarových aktiv, které patří do předmětu SAM	Jména pracovníků pro identifikaci správcovství; počty pracovníků pro účely správy licencí (pokud je to pro správu nutné); infrastruktura nebo architektura IT (včetně rozhraní), pokud je nutná pro správné použití některých licenčních ukazatelů, např. identifikace multilicencí
	Neaplikovatelná na charakteristiky, které nejsou nezbytné pro použití nebo správu softwarových aktiv, které patří do předmětu SAM	Ostatní osobní údaje

1.3 Omezení

Tato část ISO/IEC 19770 nepopisuje podrobně procesy SAM ve smyslu metod nebo postupů potřebných k plnění požadavků na výstupy procesů.

Tato část ISO/IEC 19770 nespecifikuje pořadí kroků, které by organizace měla dodržet při implementaci SAM. Toto pořadí není ani naznačováno pořadím popisu procesů. Relevantní pořadí je založeno pouze na obsahu a kontextu. Například plánování by mělo předcházet implementaci.

Tato část ISO/IEC 19770 podrobně nepopisuje dokumentaci ve smyslu názvu, formátu, přesného

obsahu a záznamového média.

Podrobnosti týkající se certifikačních schémat jsou mimo předmět této části ISO/IEC 19770.

Tato část ISO/IEC 19770 nemá být v konfliktu s jakýmkoli politikami, postupy a standardy organizací, ani s mezinárodními předpisy. Jakýkoli takový konflikt by měl být před použitím této části ISO/IEC 19770 vyřešen.

Konec náhledu - text dále pokračuje v placené verzi ČSN.