ČESKÁ TECHNICKÁ NORMA

ICS 47.020.99 **Červen 2010**

Specifikace pro systémy managementu bezpečnosti dodavatelských řetězců

ČSN
ISO 28000
01 0381

Specification for security management systems for the supply chain

Spécifications pour les systemes de management de la sureté pour la chaîne d,approvisionnement

Tato norma je českou verzí mezinárodní normy ISO 28000:2007. 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 28000:2007. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Souvisící ČSN

ČSN EN ISO 9001:2009 (01 0321) Systémy managementu kvality – Požadavky

ČSN EN ISO 14001:2005 (01 0901) Systémy environmentálního managementu – Požadavky s návodem pro použití

ČSN EN ISO 19011:2003 (01 0330) Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu

Vysvětlivky k textu převzaté normy

Termín „security“ byl schválen TNK 6 překládat v návrhu ČSN ISO 31000 jako „zabezpečení“, protože se v této normě týká ochrany před vlivy okolí na zařízení (tyto vlivy mohou být i úmyslné). Termín „safety“ tato komise doporučila překládat jako „bezpečnost“, protože se týká ochrany před vlivy zařízení na okolí (obsluhu, životní prostředí), které jsou vždy neúmyslné. V této normě ale odborná veřejnost schválila překládat termín „security“ jako „bezpečnost“, který ÚNMZ schválil. Stejně je tento termín překládán v normách ČSN EN 15602, ČSN ISO/IEC 27001, ČSN ISO/IEC 27005 a ČSN ISO/IEC 27006.

Upozornění na národní poznámky

Do normy byly k příloze A doplněny informativní národní poznámky.

Upozornění na národní přílohu

Do této normy byla doplněna národní příloha NA (informativní), která obsahuje informaci o způsobilosti k auditování shody s požadavky této normy.

Vypracování normy

Zpracovatel: Asociace technických bezpečnostních služeb Gremium Alarm, o. s., Centrum technické normalizace pro bezpečnostní služby IČ 63839911, ve spolupráci s ASIS International Česká republika, Lukáš Moravec
a Ing. Miroslav Urban

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Lubomír Drápal, CSc.

MEZINÁRODNÍ NORMA

Specifikace pro systémy managementu ISO 28000
bezpečnosti dodavatelských řetězců První vydání
2007-09-15

ICS 47.020.99

Obsah

Strana

Předmluva 5
Úvod 6
1 Předmět 9
2 Citované normativní dokumenty 9
3 Termíny a definice 9
4 Prvky systému managementu 12
4.1 Všeobecné požadavky 13
4.2 Politika managementu bezpečnosti 13
4.3 Posuzování bezpečnostních rizik a plánování 14
4.4 Zavedení a provoz 16
4.5 Kontrola a nápravná opatření 20
4.6 Přezkoumání systému managementu a neustálé zlepšování 23
Příloha A (informativní) Vztah mezi ISO 28000:2007, ISO 14001:2004 a ISO 9001:2000 24

Bibliografie 30

Contents

Page

Foreword 5
Introduction 6
1 Scope 9
2 Normative references 9
3 Terms and definitions 9
4 Security management system elements 12
4.1 General requirements 13
4.2 Security management policy 13
4.3 Security risk assessment and planning 14
4.4 Implementation and operation 16
4.5 Checking and corrective action 20
4.6 Management review and continual improvement 23
Annex A (informative) Correspondence between ISO 28000:2007, ISO 14001:2004 and ISO 9001:2000 27
Bibliograhy 30

Published in Switzerland

Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětovou federací národních normalizačních orgánů (členů ISO). Mezinárodní normy obvykle připravují 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 mezinárodní organizace, s nimiž ISO navázala pracovní styk. ISO úzce spolupracuje s Mezinárodní elektrotechnickou komisí (IEC) ve všech záležitostech normalizace v elektrotechnice.

Mezinárodní normy se navrhují v souladu s pravidly uvedenými v části 2 směrnic ISO/IEC.

Hlavním úkolem technických komisí je připravovat mezinárodní normy. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají členským orgánům k hlasování. Zveřejnění mezinárodní normy vyžaduje schválení alespoň 75 % hlasujících členů.

Upozorňuje se na možnost, že některé části tohoto dokumentu mohou být předmětem patentových práv. ISO není odpovědná za identifikování jakýchkoli nebo všech těchto patentových práv.

ISO 28000 byla vypracována ve spolupráci s technickou komisí ISO/TC 8 *Lodě a lodní technika* ve spolupráci s dalšími technickými komisemi odpovědnými za články dodavatelského řetězce.

Toto první vydání ISO 28000 ruší a nahrazuje ISO/PAS 28000:2005, která byla technicky revidována.

Úvod

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 28000 was prepared by Technical Committee ISO/TC 8, Ships and marine technology, in collaboration with other relevant technical committees responsible for specific nodes of the supply chain.

This first edition of ISO 28000 cancels and replaces ISO/PAS 28000:2005, which has been technically revised.

Introduction

Tato mezinárodní norma byla vytvořena jako odpověď na poptávku průmyslu po standardu řízení bezpečnosti. Jeho hlavním cílem je zlepšení bezpečnosti dodavatelského řetězce. Jedná se o tzv. high-level (vysokoúrovňový) standard, který umožňuje organizaci vytvořit komplexní systém managementu bezpečnosti dodavatelského řetězce. To vyžaduje, aby organizace zhodnotila bezpečnostní prostředí, ve kterém funguje, rozhodla, zda jsou přijata adekvátní bezpečnostní opatření a posoudila, zda splňuje existující správní požadavky. Jsou-li takovým procesem identifikovány veškeré potřeby bezpečnosti, organizace má zavést takové mechanismy a procesy, které takové potřeby naplní. Vzhledem k tomu, že dodavatelské řetězce jsou ve své podstatě dynamické organizace řídicí více dodavatelských řetězců, mohou vyžadovat (a kontrolovat) své dodavatele služeb, zda splňují zákonné předpisy nebo ISO normy, jako podmínku zařazení do takových dodavatelských řetězců, aby zjednodušily management bezpečnosti, jak to ukazuje obrázek 1.

This International Standard has been developed in response to demand from industry for a security management standard. Its ultimate objective is to improve the security of supply chains. It is a high-level management standard that enables an organization to establish an overall supply chain security management system. It requires the organization to assess the security environment in which it operates and to determine if adequate security measures are in place and if other regulatory requirements already exist with which the organization complies. If security needs are identified by this process, the organization should implement mechanisms and processes to meet these needs. Since supply chains are dynamic in nature, some organizations managing multiple supply chains may look to their service providers to meet related governmental or ISO supply chain security standards as a condition of being included in that supply chain in order to simplify security management as illustrated in Figure 1

Tato mezinárodní norma je aplikovatelná v případech, kdy je třeba dodavatelský řetězec organizace řídit bezpečným způsobem. Formální přístup k managementu bezpečnosti může přímo přispět ke zvýšení obchodních schopností a vyšší kredibilitě organizace.

This International Standard is intended to apply in cases where an organization,s supply chains are required to be managed in a secure manner. A formal approach to security management can contribute directly to the business capability and credibility of the organization.

Soulad s mezinárodní normou ve své podstatě neuděluje imunitu proti zákonným závazkům (neumožňuje nedodržovat zákonné požadavky). Organizace, které si přejí prokázat shodu svých vlastních systémů managementu bezpečnosti s touto normou, tak mají činit prostřednictvím nezávislých interních a externích auditů.

Compliance with an International Standard does not in itself confer immunity from legal obligations. For organizations that so wish, compliance of the security management system with this International Standard may be verified by an external or internal auditing process.

Tato mezinárodní norma je založena na struktuře ISO přijaté v ISO 14001:2004 vzhledem k tomu, že riziko v ISO 14001 je založeno na přístupu k systémům managementu. Nicméně organizace, které používají ve svých systémech managementu procesní přístup (např. ISO 9001:2000), mohou použít existující systém managementu jako základ pro vytvoření systému managementu bezpečnosti jak předepisuje tato norma.

This International Standard is based on the ISO format adopted by ISO 14001:2004 because of its risk based approach to management systems. However, organizations that have adopted a process approach to management systems (e.g. ISO 9001:2000) may be able to use their existing management system as a foundation for a security management system as prescribed in this International Standard.

Cílem této mezinárodní normy není zdvojovat jakékoliv vládní (zákonné) požadavky, nebo požadavky jiných norem, které jsou již v organizaci certifikovány, nebo již bylo ověřeno, že organizace je s nimi ve shodě. K ověření shody může být použito prvních, druhých i třetích stran (organizací).

It is not the intention of this International Standard to duplicate governmental requirements and standards regarding supply chain security management to which the organization has already been certified or verified compliant. Verification may be by an acceptable first, second, or third party organization.

POZNÁMKA Tato mezinárodní norma je založena na metodice známé jako Plánuj-Dělej-Kontroluj-Jednej (Plan-Do-Check-Act). PDCA může být popsána takto.

NOTE This International Standard is based on the methodology known as Plan-Do-Check-Act (PDCA). PDCA can be described as follows.

• Plánuj: stanov cíle a procesy nutné pro dosažení výsledků v souladu s bezpečnostní politikou organizace.

Plan: establish the objectives and processes necessary to deliver results in accordance with the organization,s security policy.

Dělej: zaveď procesy.

Do: implement the processes.

Kontroluj: monitoruj a měř procesy ve vztahu k bezpečnostní politice, cílům, cílovým hodnotám, právním a dalším požadavkům, a podávej zprávy o výsledcích.

Check: monitor and measure processes against security policy, objectives, targets, legal and other requirements, and report results.

Jednej: prováděj opatření k neustálému zlepšování výkonnosti systému managementu bezpečnosti.

Act: take actions to continually improve performance of the security management system.

1 Předmět

1 Scope

Tato mezinárodní norma specifikuje požadavky na systém managementu bezpečnosti, přičemž zahrnuje kritické aspekty pro zajištění bezpečnosti dodavatelského řetězce. Management bezpečnosti je spojen s celou řadou dalších aspektů řízení obchodní činnosti (business management). Tyto aspekty zahrnují veškeré činnosti, jež organizace provádí, řídí a mají dopad na bezpečnost dodavatelského řetězce. Ostatní aspekty mají být zvažovány ve smyslu kde a kdy mají vliv na management bezpečnosti, přičemž má být zahrnuta i přeprava produktů v rámci dodavatelského řetězce.

This International Standard specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. Security management is linked to many other aspects of business management. Aspects include all activities controlled or influenced by organizations that impact on supply chain security. These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain.

Tato norma je aplikovatelná pro jakoukoliv velikost organizací, od malých po mezinárodní, ve výrobě, službách, skladování nebo dopravě, v jakékoliv fázi produkce nebo dodavatelském řetězci, které si přejí:

1. vytvořit, zavést, udržovat a zlepšovat systém managementu bezpečnosti;

3. zajistit shodu se stanoveným managementem bezpečnosti;

4. prokázat takovou shodu ostatním;

5. usilovat o certifikaci/registraci jejího systému managementu bezpečnosti u akreditovaných certifikačních orgánů, resp. třetích stran; nebo

6. vyhlašovat resp. deklarovat shodu svého systému managementu bezpečnosti s touto mezinárodní normou.

Existují právní a správní požadavky, které se zaměřují na některé požadavky této mezinárodní normy.

Záměrem této mezinárodní normy není vyžadovat duplicitní prokazování shody s požadavky.

Organizace, které si zvolí certifikaci prostřednictvím třetí strany, mohou dále prokázat, že zásadním způsobem přispívají k bezpečnosti dodavatelského řetězce.

This International Standard is applicable to all sizes of organizations, from small to multinational, in manufacturing, service, storage or transportation a tany stage of the production or supply chain that wishwe to:

1. establish, implement, maintain and improve a security management system;

3. assure conformance with stated security management policy;

4. demonstrate such conformance to others;

5. seek certification/registration of its security management system by an Accredited third party Certification Body; or

6. make a self-determination and self-declaration of conformance with this International Standard.

There are legislative and regulatory codes that address some of the requirements in this International Standard.

It is not the intention of this International Standard to require duplicative demonstration of conformance.

Organizations that choose third party certification can further demonstrate that they are contributing significantly to supply chain security.