Část IS

Implementace v organizacích schválených dle Části-145

Modrá stodola 27.3. 2024

Zpracoval Ing. Jan Steklý

Nařízení Evropského parlamentu a Rady (EU)

NAŘÍZENÍ (EU) č. 2018/1139 ze dne 4. července 2018 o společných pravidlech v oblasti civilního letectví kterým se mění nařízení (ES) č. 2111/2005,(ES) č.1008/2008, (EU) č.996/2010 a (EU) č. 376/2014

Oblast působnosti:

Pro organizace (včetně fyzických osob) působící při projektování, výrobě, řízení zachování letové způsobilosti nebo údržbě

Dle typu prováděné činnosti a velikosti organizace zavést a udržovat systém řízení, který zajišťuje soulad s hlavními požadavky v příloh tohoto nařízení , řídit bezpečností rizika a usilovat o trvalé zdokonalování tohoto systému.

Prováděcí Nařízení komise (EU) 2023/203 ze dne 27. října 2022.

Oblast působnosti:

a) organizace údržby, na které se vztahuje oddíl A přílohy II (část 145) nařízení (EU) č. 1321/2014, s výjimkou těch, které se zabývají výhradně údržbou letadel v souladu s přílohou Vb (část ML) nařízení Komise (EU) č. 1321/2014

Prováděcí Nařízení komise (EU) 2023/203 pokračování

Prováděcí Nařízení komise (EU) 2023/203 ze dne 27. října 2022.

Toto nařízení stanoví požadavky, které musí organizace a příslušné orgány splnit s cílem:

a) **identifikovat a řídit rizika** v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví, která by mohla ovlivnit systémy a údaje informačních a komunikačních technologií používaných pro účely civilního letectví;

b) **zjistit události v oblasti bezpečnosti informací** a určit ty, které jsou považovány za incidenty v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví;

c) **reagovat na tyto incidenty** v oblasti bezpečnosti informací a zotavit se z nich

DEFINICE

„bezpečností informací“ zachování důvěrnosti, integrity, autenticity a dostupnosti sítí a informačních systémů;

„událostí bezpečnosti informací“ zjištěný výskyt stavu systému, služby nebo sítě, který poukazuje na možné narušení politiky bezpečnosti informací nebo na selhání kontrol bezpečnosti informací, nebo předem neznámá situace, která může být významná pro bezpečnost informací;

„incidentem“ jakákoliv událost, která má reálný negativní dopad na bezpečnost sítí a informačních systémů ve smyslu čl. 4 bodu 7 směrnice (EU) 2016/1148;

„rizikem bezpečnosti informací“ riziko pro organizační provoz civilního letectví, aktiva, jednotlivce a jiné organizace v důsledku potenciálu události bezpečnosti informací. Rizika bezpečnosti informací jsou spojena s potenciální možností, že hrozby zneužijí zranitelností informačního aktiva nebo skupiny informačních aktiv

Prováděcí Nařízení komise (EU) 2023/203 pokračování

Článek 4 Požadavky na organizace a příslušné orgány

1. Organizace uvedené v čl. 2 odst. 1 musí splňovat požadavky přílohy II (část IS.I.OR) tohoto nařízení tj. pro AMO dle Části -145

Článek 12 Změna nařízení (EU) č. 1321/2014

Přílohy II (část 145), III (část 66) a Vc (část CAMO) nařízení (EU) č. 1321/2014 se mění v souladu s přílohou VII tohoto nařízení.

Článek 16

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v Úředním věstníku Evropské unie tj. od 22.února 2023

Použije se od 22. února 2026.

Změny nařízení (EU) č. 1321/2014 Část 145

1) Příloha II (část 145) se mění takto :

a) Obsah se mění takto

i) za nadpis 145.A.200 se vkládá nový nadpis, který zní:
„145.A.200A Systém řízení bezpečnosti informací“;

b) za bod 145.A.200 se vkládá nový bod 145.A.200A, který zní:

„145.A.200A **Systém řízení bezpečnosti informací**

Kromě systému řízení uvedeného v bodě 145.A.200 organizace údržby zavede, uplatňuje a udržuje systém řízení bezpečnosti informací v souladu s prováděcím nařízením (EU) 2023/203, aby bylo zajištěno řádné řízení rizik bezpečnosti informací, která mohou mít dopad na bezpečnost letectví.“

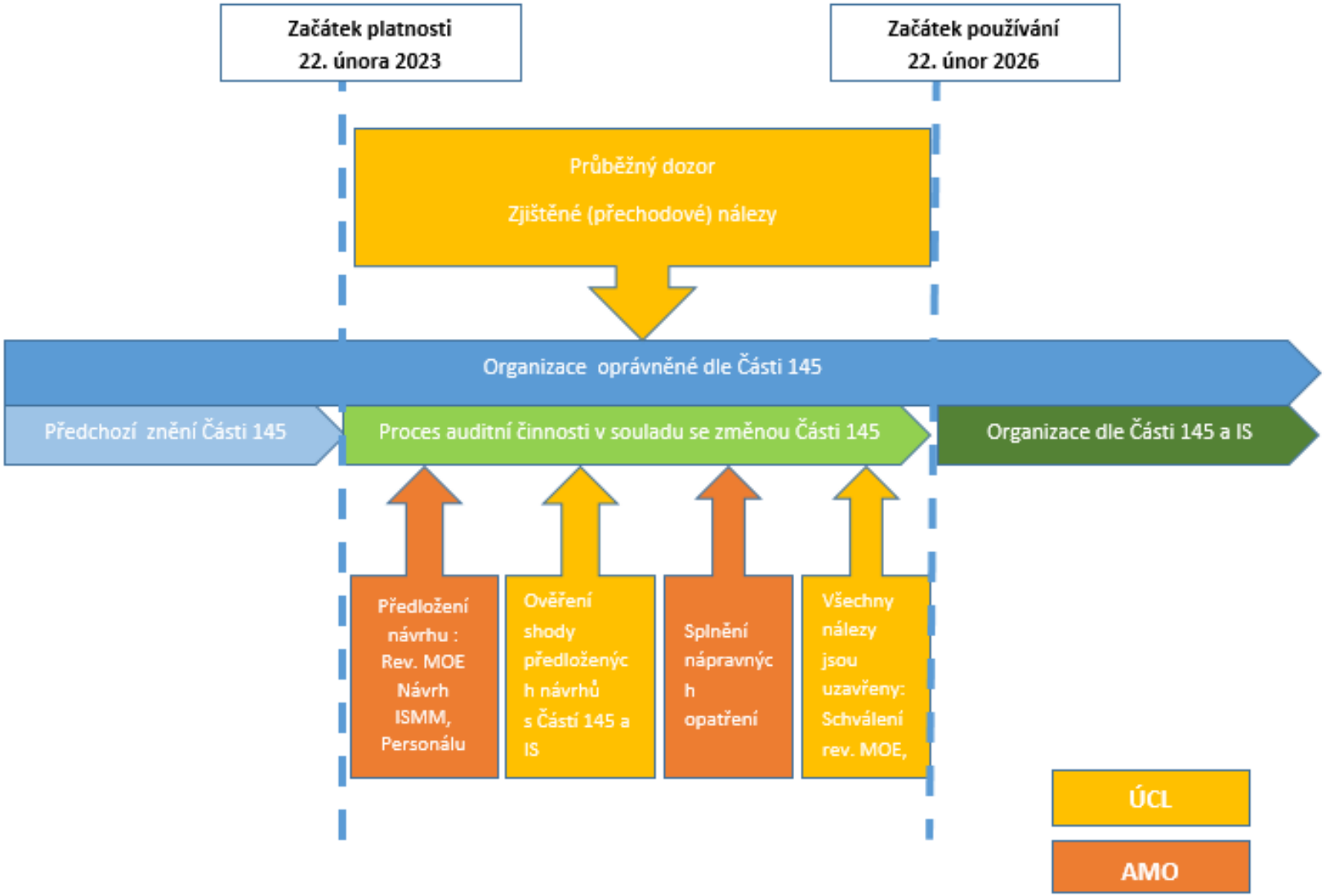
ČÁST-IS.I.OR Bezpečnost informací-požadavky organizace

IS.I.OR.200 Systém řízení bezpečnosti informací (ISMS)

a) Za účelem dosažení cílů stanovených v článku 1 organizace vytvoří, zavede a udržuje systém řízení bezpečnosti informací (ISMS), který zajistí, že organizace:

1) ***stanoví politiku bezpečnosti informací***
2) ***identifikuje a přezkoumává rizika*** bezpečnosti informací
3) ***definuje a provádí opatření k řešení rizik*** bezpečnosti informací
4) ***zavede systém interního hlášení*** v oblasti bezpečnosti informací
5) ***definuje a provede opatření*** potřebná k odhalování událostí v oblasti bezpečnosti informací, určuje události, které jsou považovány za incidenty s možným dopadem na bezpečnost letectví, reaguje na tyto incidenty v oblasti bezpečnosti informací a odstraňuje jejich následky;
6)***provádí opatření***, která příslušný orgán oznámil *jako* ***okamžitou reakci*** na incident nebo zranitelnost v oblasti bezpečnosti informací s dopadem na bezpečnost letectví
7) ***přijme vhodná opatření*** k řešení zjištění oznámených příslušným orgánem
8) ***zavede systém externího hlášení***, aby mohl příslušný orgán přijmout vhodná opatření;
9) dodržuje požadavky obsažené v bodě IS.I.OR.235, pokud zadává jakoukoliv část činností uvedených v bod IS.I.OR.200 jiným organizacím

Zavedení IS v organizacích schválených dle Part-145



Zavedení IS v organizacích schválených dle Part-145

Organizace, které nemají osvědčení dle Part-145

Organizace, které požádají o osvědčení o oprávnění dle Part-145 po 22.2.2026 již musí postupovat podle ustanovení daných Prováděcím nařízení (EU) č. 2023/203.

Organizace, které jsou držiteli osvědčení dle Part-145

Během „přechodného období“ tj. v období do 22.2.2026 ÚCL provádí průběžný dohled.

Když jsou zjištěny neshody s Částí-145 respektive IS, inspektor udělí lhůtu pro splnění nápravných opatření související s typem nálezu. „Přechodné nálezy“ mohou mít prováděcí období delší než běžné období 3 měsíců, ale tyto nálezy musí být uzavřeny (včetně schválení) do 22. února 2026.

Zavedení IS v organizacích schválených dle Part-145 pokračování Části IS.I.OR.200

10) ***splňuje požadavky na zaměstnance*** stanovené v bodě IS.I.OR.240;
11) ***splňuje požadavky na vedení záznamů*** stanovené v bodě IS.I.OR.245;
12) ***sleduje, jak organizace plní požadavky tohoto nařízení a poskytuje zpětnou vazbu o zjištěních odpovědnému vedoucímu pracovníkovi, aby zajistil účinné provádění nápravných opatření;***
13) ***chrání,*** aniž by byly dotčeny platné požadavky na hlášení incidentů, ***důvěrnost všech informací,*** které organizace mohla obdržet od jiných organizací, a to podle úrovně jejich citlivosti

b) Za účelem trvalého plnění požadavků uvedených v článku 1 musí organizace zavést proces trvalého zlepšování v souladu s bodem IS.I.OR.260.

c) Organizace musí v souladu s bodem IS.I.OR.250 zdokumentovat všechny klíčové procesy, postupy, role a odpovědnosti požadované pro splnění bodu IS.I.OR.200 písm. a) a musí zavést proces pro změnu této dokumentace. Změny těchto procesů, postupů, rolí a odpovědností se řídí podle bodu IS.I.OR.255.

d) Procesy, postupy, úlohy a povinnosti zavedené organizací za účelem dosažení souladu s bodem IS.I.OR.200 písm. a) musí odpovídat povaze a složitosti jejích činností na základě posouzení rizik bezpečnosti informací spojených s uvedenými činnostmi a mohou být začleněny do jiných stávajících systémů řízení, které již organizace provádí.

e) Aniž je dotčena povinnost dodržovat požadavky týkající se hlášení uvedené v nařízení (EU) č. 376/2014 a požadavky bodu IS.I.OR.200 písm. a) bodu 13, může příslušný úřad organizaci udělit oprávnění neprovádět požadavky uvedené v písmenech a) až d) a související požadavky uvedené v bodech IS.I.OR.205 až IS.I.OR.260, pokud ke spokojenosti uvedeného úřadu prokáže, že její činnosti, zařízení a zdroje, jakož i služby, které provozuje, poskytuje, přijímá a udržuje, nepředstavují ani pro ni, ani pro jiné organizace žádná rizika bezpečnosti informací s potenciálním dopadem na bezpečnost letectví.

Zavedení IS v organizacích schválených dle Part-145

Schválení musí vycházet z dokumentovaného posouzení rizik bezpečnosti informací, které provede organizace nebo třetí strana v souladu s bodem IS.I.OR.205 a které přezkoumá a schválí její příslušný orgán tj. ÚCL.

Platnost tohoto schválení bude přezkoumána ÚCL v návaznosti na příslušný cyklus dozorových auditů a vždy, když dojde ke změnám v rozsahu činnosti organizace AMO.

IS.I.OR.205 Posouzení rizik bezpečnosti informací

a) *Organizace identifikuje všechny své prvky*, které by mohly být vystaveny rizikům bezpečnosti informací. Patří sem:

1. činnosti, zařízení a zdroje organizace, jakož i služby, které organizace provozuje, poskytuje, přijímá nebo udržuje;

2. vybavení, systémy, údaje a informace, které přispívají k fungování prvků uvedených v bodě 1.

b) *Organizace identifikuje rozhraní*, která má s jinými organizacemi a která by mohla vést k vzájemné expozici rizikům v oblasti bezpečnosti informací

Zavedení IS v organizacích schválených dle Part-145

c) S ohledem na prvky a rozhraní uvedené v písmenech a) a b) organizace identifikuje rizika v oblasti bezpečnosti informací, která mohou mít možný dopad na bezpečnost letectví.

d) Organizace přezkoumá a aktualizuje posouzení rizik

IS.I.OR.210 Řešení rizik bezpečnosti informací

a) Organizace vypracuje opatření k řešení nepřijatelných rizik zjištěných v souladu s bodem IS.I.OR.205, včas je provede a kontroluje jejich trvalou účinnost. Tato opatření musí organizaci umožnit:

1)*kontrolovat okolnosti*, které přispívají ke skutečnému výskytu scénáře hrozeb;

2) *snížit důsledky* pro bezpečnost letectví spojené s naplněním scénáře hrozeb;

3) *vyhnout se rizikům*. Tato opatření nesmí přinést žádná nová možná nepřijatelná rizika pro bezpečnost letectví.

b) AM a ostatní dotčení pracovníci organizace musí být informováni o výsledku posouzení rizik provedeného v souladu s bodem IS.I.OR.205, o odpovídajících scénářích hrozeb a o opatřeních, která mají být provedena. Organizace rovněž informuje organizace, s nimiž má rozhraní v souladu s bodem IS.I.OR.205 písm. b), o všech rizicích sdílených mezi oběma organizacemi

Zavedení IS v organizacích schválených dle Part-145

IS.I.OR.215 Systém interního hlášení v oblasti bezpečnosti informací

Organizace vytvoří systém interního hlášení, který umožní shromažďování a vyhodnocování událostí v oblasti bezpečnosti informací.

Každá smluvní organizace, která může organizaci vystavit rizikům v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví*, je povinna této organizaci hlásit události v oblasti bezpečnosti informací.*

Organizace spolupracuje při vyšetřování s jakoukoli jinou organizací, která významně přispívá k bezpečnosti informací v rámci své vlastní činnosti.

Organizace může tento systém podávání hlášení integrovat s jinými systémy podávání hlášení, které již zavedla

Zavedení IS v organizacích schválených dle Part-145

IS.I.OR.220 Incidenty bezpečnosti informací – odhalení, reakce a zotavení

a) Na základě výsledku posouzení rizik provedeného podle bodu IS.I.OR.205 a výsledku ošetření rizik provedeného podle bodu IS.I.OR.210 organizace provede *opatření k odhalování incidentů a zranitelností*, které naznačují možné naplnění nepřijatelných rizik a které mohou mít možný dopad na bezpečnost letectví.

b) Organizace zavede *opatření, která reagují na všechny podmínky* události zjištěné v souladu s písmenem a), které se mohou rozvinout nebo se rozvinuly do incidentu v oblasti bezpečnosti informací.

c) Organizace zavede *opatření zaměřená na obnovu po incidentech* v oblasti bezpečnosti informací, včetně případných mimořádných opatření.

Zavedení IS v organizacích schválených dle Part-145

IS.I.OR.225 Reakce na zjištění oznámená příslušným orgánem

a) Po obdržení oznámení o zjištěních předloženého příslušným orgánem organizace: 1) zjistí hlavní příčinu nebo příčiny nesouladu a faktory, které k němu přispěly; 2) vytvoří plán nápravných opatření; 3) prokáže nápravu nesouladu ke spokojenosti příslušného orgánu
b) Opatření uvedená v písmenu a) se provedou ve lhůtě dohodnuté s příslušným orgánem

IS.I.OR.230 Systém externího hlášení v oblasti bezpečnosti informací

a) Organizace zavede systém podávání hlášení o bezpečnosti informací, který splňuje požadavky stanovené v nařízení (EU) č. 376/2014 a jeho aktech v přenesené pravomoci a prováděcích aktech, pokud se toto nařízení na organizaci vztahuje.
b) Aniž jsou dotčeny povinnosti vyplývající z nařízení (EU) č. 376/2014, organizace zajistí, aby každý incident nebo zranitelnost v oblasti bezpečnosti informací, které mohou představovat významné riziko pro bezpečnost letectví, byly oznámeny jejich příslušnému orgánu.

Zavedení IS v organizacích schválených dle Part-145

IS.I.OR.235 Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací

Organizace zajistí, aby při zadávání jakékoli části činností jiným organizacím byly zadané činnosti v souladu s požadavky tohoto nařízení a aby organizace provádějící zadání *pracovala pod jejím dozorem a rizika spojená se smluvními činnostmi byla náležitě řízena*.

Organizace zajistí, aby příslušný orgán mohl mít na požádání přístup do smluvní organizace, a mohl tak zjistit, zda jsou nadále plněny příslušné požadavky stanovené v tomto nařízení

IS.I.OR.240 Požadavky na personál

AM -

1) zajistí, aby byly k dispozici veškeré zdroje nezbytné ke splnění požadavků tohoto nařízení;

2) zavede a podporuje politiku bezpečnosti informací

3) prokáže základní porozumění tomuto nařízení.

Zavedení IS v organizacích schválených dle Part-145

AM - jmenuje osobu nebo skupinu osob, které zajistí, aby organizace splňovala požadavky tohoto nařízení, a vymezí rozsah jejich pravomoci. Tato osoba (nebo skupina osob) je podřízena přímo odpovědnému vedoucímu a má odpovídající znalosti, kvalifikaci a zkušenosti k plnění svých povinností. V postupech je určeno, kdo zastupuje určitou osobu v případě její dlouhodobé nepřítomnosti.

jmenuje osobu nebo skupinu osob s odpovědností za řízení funkce sledování souladu uvedené v bodě IS.I.OR.200 písm. a) bodě 12.

Pokud organizace sdílí organizační struktury, politiky, procesy a postupy v oblasti bezpečnosti informací s jinými organizacemi nebo s částmi své vlastní organizace, na něž se nevztahuje oprávnění nebo prohlášení, může odpovědný vedoucí pověřit společnou odpovědnou osobu.

V takovém případě se stanoví koordinační opatření mezi odpovědným vedoucím organizace a společnou odpovědnou osobou s cílem zajistit odpovídající integraci řízení bezpečnosti informací v rámci organizace.
Organizace musí mít zavedeny procesy, které zajistí, aby měla ve službě dostatečný počet pracovníků s nezbytnou způsobilostí, pravomocemi a zavede procesy, které zajistí, aby pracovníci měli k plnění svých úkol přístup k informačním systémům a údajům na základě prokázání jejich totožnosti a důvěryhodnosti.

Zavedení IS v organizacích schválených dle Part-145

IS.I.OR.245 Vedení záznamů

a) Organizace vede záznamy o svých činnostech v oblasti řízení bezpečnosti informací a archivuje nejméně 5 let

b) Organizace vede záznamy o kvalifikaci a zkušenostech vlastních zaměstnanců zapojených do činností řízení bezpečnosti informací

c) Formát záznamů je upřesněn v postupech organizace.

d) Záznamy jsou uchovávány způsobem zajišťujícím jejich ochranu před poškozením, pozměňováním a krádeží, přičemž informace se, je-li to vyžadováno, identifikují podle svého stupně utajení. Organizace zajistí, aby záznamy byly uchovávány za použití prostředků, které zajistí integritu, pravost a oprávněný přístup.

Zavedení IS v organizacích schválených dle Part-145

IS.I.OR.250 Příručka pro řízení bezpečnosti informací (ISMM)

a) Organizace vydá příručku pro řízení bezpečnosti informací (ISMM) která obsahuje:
1) prohlášení podepsané AM, kterým se potvrzuje, že organizace bude svou činnost vždy vykonávat v souladu s touto přílohou a příručkou ISMM. Pokud AM není statutárním organizace, musí prohlášení spolupodepsat statutární zástupce;
2) funkci (funkce), jméno (jména), úkoly, odpovědnosti, povinnosti a pravomoci osoby či osob uvedených v bodě IS.I.OR.240 písm. b) a c);
3) v příslušných případech funkci, jméno, úkoly, odpovědnosti, povinnosti a pravomoc společné odpovědné osoby definované v bodě IS.I.OR.240 písm. d);
4) politiku bezpečnosti informací organizace uvedenou v bodě IS.I.OR.200 písm.a) bodě 1;
5) obecný popis počtu a kategorií pracovníků a zavedeného systému plánování dostupnosti pracovníků, jak je požadováno v bodě IS.I.OR.240;
6) funkci (funkce), jméno (jména), úkoly, odpovědnosti, povinnosti a pravomoci klíčových osob odpovědných za provádění bodu IS.I.OR.200, včetně osoby nebo osob odpovědných za funkci sledování souladu
7) organizační schéma znázorňující související odpovědnostní vztahy mezi osobami
8) popis systému interního hlášení
9) postupy upřesňující jak organizace zajišťuje soulad s Částí IS
10) podrobnosti o aktuálně schválených alternativních způsobech plnění předpisů.

Zavedení IS v organizacích schválených dle Part-145

b) První vydání příručky řízení bezpečnosti informací schvaluje a kopii si ponechá ÚCL. Příručka řízení bezpečnosti informací se mění podle potřeby tak, aby byla vždy aktuálním popisem systému ISMS organizace. Kopie všech změn příručky ISMM se poskytne ÚCL.

c) Změny příručky ISMM se řídí postupem stanoveným organizací. Změny, které nespadají do oblasti působnosti tohoto postupu, a změny týkající se změn uvedených v bodě IS.I.OR.255 písm. b) schvaluje ÚCL.

d) Organizace může integrovat příručku ISMM s jinými výklady organizace nebo příručkami managementu, které má k dispozici, za předpokladu, že existuje jasný křížový odkaz, který uvádí, které části výkladu nebo příručky managementu odpovídají jednotlivým požadavkům obsaženým v příloze.II, Části IS.

Zavedení IS v organizacích schválených dle Part-145

IS.I.OR.255 Změny systému řízení bezpečnosti informací

a) Změny systému ISMS mohou být řízeny a oznamovány ÚCL postupem, který organizace vypracuje. Tento postup schvaluje ÚCL.

b) Pokud jde o změny systému ISMS, na které se nevztahuje postup uvedený v písmenu a), musí organizace požádat o schválení vydané ÚCL a získat ho. Pokud jde o tyto změny potom platí:

   1) Žádost o provedení změny musí být podána předtím, než k jakýmkoli takovým změnám dojde, aby příslušný orgán mohl určit, zda budou i nadále dodrženy požadavky tohoto nařízení a aby v případě potřeby mohl změnit osvědčení organizace a s ním spojené podmínky schválení;

   2) organizace poskytne příslušnému orgánu veškeré informace, které si vyžádá k posouzení změny;

   3) změna se provede až po získání formálního schválení příslušným orgánem;

   4) během provádění těchto změn bude organizace svou činnost provozovat v souladu s platnými podmínkami, které jí příslušný orgán stanovil.

Zavedení IS v organizacích schválených dle Part-145

IS.I.OR.260 Soustavné zlepšování

a) Organizace musí pomocí vhodných ukazatelů výkonnosti hodnotit účinnost a vyspělost systému ISMS. Toto hodnocení se provádí na kalendářním základě předem stanoveném organizací nebo po incidentu v oblasti bezpečnosti informací.

b) Pokud jsou po posouzení provedeném podle písmene a) zjištěny nedostatky, přijme organizace nezbytná opatření ke zlepšení, aby zajistila, že systém ISMS bude i nadále splňovat platné požadavky a udrží rizika bezpečnosti informací na přijatelné úrovni. Kromě toho organizace přehodnotí ty prvky systému ISMS, které jsou přijatými opatřeními ovlivněny.

Děkuji Vám za pozornost a na závěr informace kde naleznete více k problematice Části IS

EASA
European Union Aviation Safety Agency

Acceptable Means of Compliance and Guidance Material to Annex II (Part-IS.I.OR) to Commission Implementing Regulation (EU) 2023/203

www.easa.europa.eu/en/regulations/information-security#part-isior

Issue 1

12 July 2023[1]

First Easy Access Rules for Information Security (Regulations (EU) 2023/203 and 2022/1645) na adrese:
https://www.easa.europa.eu/en/document-library/easy-access-rules/first-easy-access-rules-information-security-regulations-eu