UPOZORNĚNÍ:

Ačkoliv jsou tyto texty doslovným překladem originálního textu rozhodnutí výkonného ředitele EASA, slouží příslušné dokumenty připravované ÚCL pouze pro informační účely a ÚCL nenese za jejich obsah odpovědnost. Tyto texty nemají žádnou právní hodnotu. Originální znění naleznete v Úřední publikaci Agentury, tj. na webových stránkách http://easa.europa.eu.

Datum aktualizace tohoto dokumentu: 2. 8. 2024

Rozhodnutí výkonného ředitele

2023/009/R

ze dne 12. července 2023

kterým se vydává následující:

1. vydání Přijatelných způsobů průkazu a poradenského materiálu k Příloze (Část IS.D.OR) k nařízení Komise v přenesené pravomoci (EU) 2022/1645

„AMC a GM k Části IS.D.OR – 1. vydání“

a

1. vydání Přijatelných způsobů průkazu a poradenského materiálu k Příloze II (Část IS.I.OR) k prováděcímu nařízení Komise (EU) 2023/203

„AMC a GM k Části IS.I.OR – 1. vydání“

— — —

„Řízení rizik v oblasti bezpečnosti informací – AMC & GM k Části IS.D.OR a Části IS.I.OR“

VÝKONNÝ ŘEDITEL AGENTURY EVROPSKÉ UNIE PRO BEZPEČNOST LETECTVÍ (EASA)

s ohledem na nařízení (EU) 2018/1139[1], a zejména na článek 76 odst. 3 a článek 104 odst. 3 písm. a) tohoto nařízení,

vzhledem k těmto důvodům:

(1) Přijatelné způsoby průkazu jsou nezávazné standardy vydané EASA, které jsou osobami a organizacemi využívány k prokázání vyhovění nařízení (EU) 2018/1139 a aktům v přenesené pravomoci a prováděcím aktům přijatým na jeho základě.

(2) Poradenský materiál je nezávazný materiál vydaný EASA, který pomáhá ilustrovat význam aktů v přenesené pravomoci nebo prováděcích aktů nebo certifikačních specifikací a podrobných specifikací a který se používá k podpoře výkladu nařízení (EU) 2018/1139, aktů v přenesené pravomoci a prováděcích aktů přijatých na jeho základě a certifikačních specifikací a podrobných specifikací.

(3) EASA je povinna, na základě článku 4 odst. 1 písm. a) nařízení (EU) 2018/1139, zohledňovat současný stav techniky a osvědčené postupy v oblasti letectví a

[1] Nařízení (EU) 2018/1139 Evropského parlamentu a Rady ze dne 4. července 2018 o společných pravidlech v oblasti civilního letectví a o zřízení Agentury Evropské unie pro bezpečnost letectví, kterým se mění nařízení (ES) č. 2111/2005, (ES) č. 1008/2008, (EU) č. 996/2010, (EU) č. 376/2014 a směrnice Evropského parlamentu a Rady 2014/30/EU a 2014/53/EU a kterým se zrušuje nařízení Evropského parlamentu a Rady (ES) č. 552/2004 a (ES) č. 216/2008 a nařízení Rady (EHS) č. 3922/91 (Úř. věst. L 212, 22.08.2018, s. 1) (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1535612134845&uri=CELEX:32018R1139).

aktualizovat svá rozhodnutí s ohledem na celosvětové zkušenosti v letectví a vědeckotechnický pokrok v daných oblastech.

(4) Nařízení Komise v přenesené pravomoci (EU) 2022/1645[2] a prováděcí nařízení Komise (EU) 2023/203[3] stanovují požadavky pro organizace a příslušné úřady týkající se řízení rizik v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví.

(5) V souvislosti s tím EASA určila potřebu vydat tento soubor přijatelných způsobů průkazu a poradenského materiálu, aby se usnadnilo provádění výše uvedených nových požadavků.

(6) EASA, v souladu s článkem 115 odst. 1 písm. c) nařízení (EU) 2018/1139 a článkem 6 postupu pro předpisovou činnost EASA[4], konzultovala své poradní orgány ohledně obsahu tohoto rozhodnutí, a obdržené připomínky zohlednila.

ROZHODL TAKTO:

Článek 1

Přijatelné způsoby průkazu a poradenský materiál k Příloze (Část IS.D.OR) k nařízení Komise v přenesené pravomoci (EU) 2022/1645 se tímto stanovují v příloze I k tomuto rozhodnutí.

Článek 2

Přijatelné způsoby průkazu a poradenský materiál k Příloze II (Část IS.I.OR) k prováděcímu nařízení Komise (EU) 2023/203 se tímto stanovují v příloze II k tomuto rozhodnutí.

Článek 3

Toto rozhodnutí vstupuje v platnost den po jeho uveřejnění v Úřední publikaci EASA.

Použije se od 22. února 2026.

V Kolíně nad Rýnem dne 12. července 2023

---

[2] Nařízení Komise v přenesené pravomoci (EU) 2022/1645 ze dne 14. července 2022, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) 2018/1139, pokud jde o požadavky na řízení rizik bezpečnosti informací s potenciálním dopadem na bezpečnost letectví pro organizace, na něž se vztahují nařízení Komise (EU) č. 748/2012 a (EU) č. 139/2014, a kterým se mění nařízení Komise (EU) č. 748/2012 a (EU) č. 139/2014 (Úř. věst. L 248, 26.09.2022, s. 18) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1645&qid=1688140452938).

[3] Prováděcí nařízení Komise (EU) 2023/203 ze dne 27. října 2022, prováděcí nařízení Komise ze dne 27. října 2022, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) 2018/1139, pokud jde o požadavky na řízení rizik v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví pro organizace, na které se vztahují nařízení Komise (EU) č. 1321/2014, (EU) č. 965/2012, (EU) č. 1178/2011, (EU) 2015/340, prováděcí nařízení Komise (EU) 2017/373 a (EU) 2021/664, a pro příslušné orgány, na které se vztahují nařízení Komise (EU) č. 748/2012, (EU) č. 1321/2014, (EU) č. 965/2012, (EU) č. 1178/2011, (EU) 2015/340 a (EU) č. 139/2014, prováděcí nařízení Komise (EU) 2017/373 a (EU) 2021/664, a kterým se mění nařízení Komise (EU) č. 1178/2011, (EU) č. 748/2012, (EU) č. 965/2012, (EU) č. 139/2014, (EU) č. 1321/2014, (EU) 2015/340 a prováděcí nařízení Komise (EU) 2017/373 a (EU) 2021/664 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R0203&qid=1687859731466).

[4] EASA je povinna dodržovat strukturovaný proces tvorby předpisů, jak je požadováno článkem 115 odst. 1 nařízení (EU) 2018/1139. Tento proces byl přijat rozhodnutím správní rady EASA (MB) a je odkazován jako „postup pro předpisovou činnost“. Viz rozhodnutí MB č. 01-2022 ze dne 2. května 2022 ohledně postupu použitého EASA při vydávání stanovisek, certifikačních specifikací a dalších podrobných specifikací, přijatelných způsobů průkazu a poradenského materiálu („postup pro předpisovou činnost“) a kterým se nahrazuje rozhodnutí správní rady č. 18-2015 (https://www.easa.europa.eu/the-agency/management-board/decisions/easa-mb-decision-no-01-2022-rulemaking-procedure-repealing-mb).

Za Agenturu Evropské unie pro bezpečnost letectví
Výkonný ředitel

Patrick KY

Přijatelné způsoby průkazu a poradenský materiál k Příloze (Část IS.D.OR) k nařízení Komise v přenesené pravomoci (EU) 2022/1645

První vydání

12. července 2023[1]

[1] Datum vstupu v platnost tohoto vydání prosím viz rozhodnutí 2023/009/R v Úřední publikaci EASA.

OBSAH

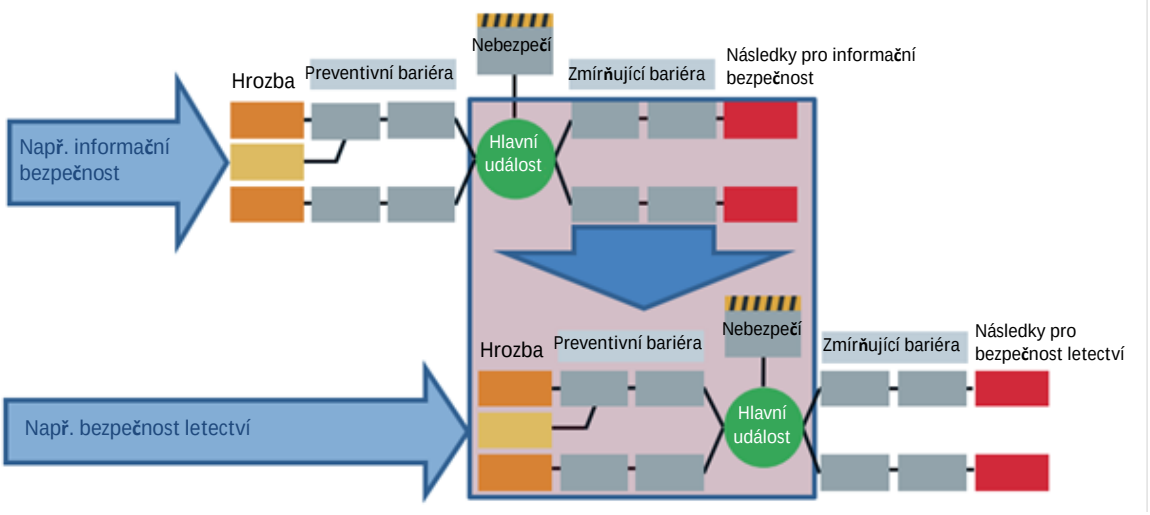
AMC A GM K PŘÍLOZE (ČÁST IS.D.OR) K NAŘÍZENÍ KOMISE V PŘENESENÉ PRAVOMOCI (EU) 2022/1645

GM1 IS.D.OR.200 Systém řízení bezpečnosti informací (ISMS)

Systém řízení bezpečnosti informací (ISMS) je systematický přístup k ustavení, implementaci, provádění, monitorování, přezkoumávání, udržování a neustálému zlepšování stavu informační bezpečnosti v rámci organizace. Jeho cílem je chránit informační aktiva tak, aby provozních a bezpečnostních cílů organizace bylo možné dosáhnout s vědomím rizik, účinným a efektivním způsobem.

Obecně řečeno, ISMS zavádí proces řízení rizik v oblasti bezpečnosti informací, na základě výsledků analýz dopadů v oblasti bezpečnosti informací, které v podstatě určují jeho rozsah. Pokud narušení bezpečnosti informací může způsobit následky pro bezpečnost letectví nebo k nim přispět, musí požadavky na zabezpečení informací omezit jejich vliv na úrovně bezpečnosti letectví, které jsou považovány za přijatelné. Všechny role, procesy nebo informační systémy, které mohou způsobit následky pro bezpečnost letectví nebo k nim přispět, tedy spadají do oblasti působnosti nařízení (EU) 2022/1645. ISMS poskytuje způsob, jak rozhodnout o potřebných opatřeních v oblasti informační bezpečnosti pro všechny architektonické vrstvy (správa a řízení, obchod, aplikace, technologie, data) a domény (organizační, lidská, fyzická, technická). Dále umožňuje řídit výběr, implementaci a provádění opatření v oblasti informační bezpečnosti. Konečně umožňuje řídit správu a řízení, řízení rizik a shodu (GRC) v rámci ISMS.

Proces řízení rizik je tedy založen na posuzováních rizik bezpečnosti letectví a odvozených úrovních přijatelnosti rizik v oblasti bezpečnosti informací, které jsou navrženy tak, aby účinně ošetřovaly a řídily rizika v oblasti bezpečnosti informací s potenciálním dopadem na bezpečnost letectví způsobená hrozbami využívajícími zranitelností informačních aktiv v leteckých systémech. Interagující motýlkové *(bow-tie)* diagramy umožňují ilustraci (na vyšší úrovni a nevyčerpávající) toho, jak může být nezbytné, aby různé obory posuzování rizika spolupracovaly, s cílem vytvořit společnou perspektivu na riziko, jak je znázorněno na obrázku 1.



Obrázek 1: Zobrazení řízení rizik v oblasti bezpečnosti letectví, která představují hrozby informační bezpečnosti, prostřednictvím motýlkového diagramu

ISMS v tomto nařízení by měl spojovat kompetence v oblasti bezpečnosti informací a bezpečnosti letectví ve většině procesů, včetně například identifikace kritických systémů nebo hrozeb a posuzování potenciálních dopadů na bezpečnost letectví a rizik pro něj.

Implementace a udržování ISMS

ISMS, jak je definován v tomto nařízení, využívá perspektivy správy a řízení, rizika a shody a přístup, který kombinuje dimenze bezpečnostního rizika a výkonnosti, aby určil opatření v oblasti bezpečnosti informací, které jsou vhodné a v souladu s konkrétním kontextem a mohou účinně poskytovat úroveň ochrany požadovanou k dosažení cílů v oblasti bezpečnosti letectví prostřednictvím:

— Hledisko **správy a řízení** se týká poskytování směru a vedení managementu s cílem dosáhnout vlastních zastřešujících cílů subjektu:

  — vedení a závazek vrcholového managementu definující a zajišťující úzké zapojení managementu a implementaci ISMS „shora dolů“

  — cíle bezpečnosti informací a bezpečnosti v souladu a konzistentní s obchodními cíli subjektu a monitorované např. přezkoumáními managementem

  — politiky informační bezpečnosti stanovující zásady a cíle, kterých má být dosaženo

  — role, odpovědnosti, kompetence a zdroje potřebné pro efektivní ISMS

  — efektivní, na cílovou skupinu orientovaná komunikace s interními a externími zainteresovanými stranami

— Hledisko **rizik** odkazuje na klíčový aspekt ISMS v kontextu bezpečnosti letectví podle tohoto nařízení a slouží jako základ pro transparentní rozhodování a stanovení priorit kontrol a možností řešení rizik. Dále se týká posuzování, řešení a monitorování rizik informační bezpečnosti na podporu řízení rizik v oblasti bezpečnosti letectví pro klíčové procesy a informační aktiva, na kterých závisí. To zahrnuje požadavky na ochranu, vystavení riziku, postoj k rizikům a kritéria přijatelnosti rizik, metody a průmyslové normy.

— Hledisko **shody** se týká souladu s regulačními, právními a smluvními požadavky. To zahrnuje:

  — toto nařízení,

  — vlastní zásady a normy subjektu a dále mohou zahrnovat mezinárodní nebo průmyslové normy převzaté subjektem od ISO, EUROCAE atd.

  Toto hledisko zahrnuje definici, implementaci a udržování požadovaných ustanovení o bezpečnosti informací, jejichž účelnost a soulad by měly být pravidelně sledovány a zajišťovány např. (interními) audity.

Na základě těchto hledisek můžeme identifikovat následující procesy a předmětové oblasti, které se ukázaly jako relevantní pro zavedení efektivního ISMS. Tyto procesy a oblasti ISMS lze shrnout takto:

(a) vytvoření kontextu definujícího rozsah, rozhraní, závislosti a požadavky zainteresovaných stran;

(b) vedení a závazek vrcholového managementu;

(c) cíle informační bezpečnosti a bezpečnosti;

(d) zásady v oblasti bezpečnosti informací;

(e) role, odpovědnosti, kompetence a zdroje potřebné pro efektivní;

(f) komunikace s interními a externími zainteresovanými stranami k dosažení dostatečné úrovně povědomí v oblasti bezpečnosti informací a školení všech zúčastněných stran;

(g) řízení rizik v oblasti bezpečnosti informací včetně posuzování a řešení rizik;

(h) řízení incidentů bezpečnosti informací zavádějící procesy pro zvládání incidentů a zranitelností v oblasti bezpečnosti informací;

(i) monitorování, měření a vyhodnocování výkonnosti a účelnosti;

(j) interní audity a přezkoumání managementem;

(k) nápravy a nápravná opatření;

(l) neustálé zlepšování;

(m) vztah s dodavateli;

(n) dokumentace, vedení záznamů a shromažďování důkazů.

Mezi další kritické faktory úspěchu pro implementaci a provádění ISMS patří:

— ISMS by měl být integrován do procesů subjektu a celkové struktury řízení nebo dokonce – alespoň částečně, se zárukami pro jejich příslušnou integritu, a pokud je to rozumně aplikovatelné – se zastřešujícím systémem řízení zahrnujícím informační bezpečnost, bezpečnost letectví a řízení kvality.

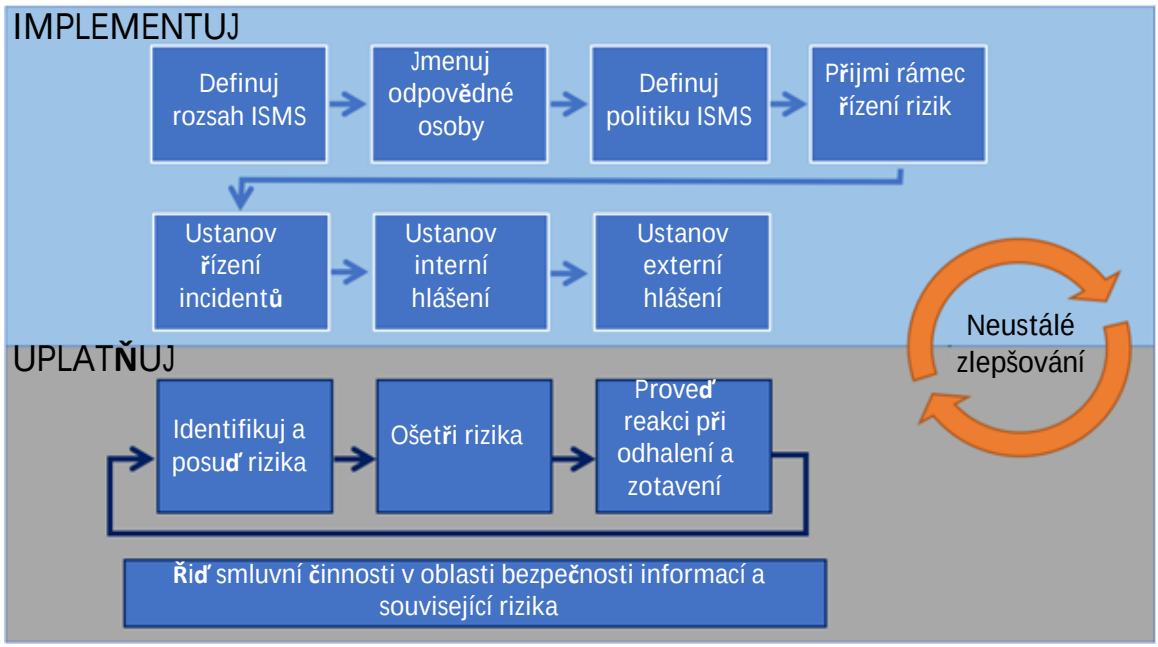
— Informační bezpečnost musí být zohledněna v rané fázi celkového návrhu procesů a postupů, systémů a opatřeních v oblasti informační bezpečnosti, aby byly hladce integrovány, aby byla zajištěna maximální účelnost, minimální funkční interference a optimalizované náklady. Žádného z těchto přínosů nelze dosáhnout pozdější integrací.

— Proces řízení rizik určuje vhodné charakteristiky preventivních opatření pro dosažení a udržení přijatelných úrovní rizik.

— Proces řízení incidentů zajišťuje, že organizace včas odhalí, reaguje a odpovídá na incidenty v oblasti informační bezpečnosti. Toho je dosaženo tím, že se předem definují odpovědnosti, postupy, scénáře a plány reakce, aby byla zajištěna koordinovaná, cílená a účinná reakce.

— Provádí se průběžné monitorování a přehodnocování a v reakci na to jsou prováděna zlepšení.

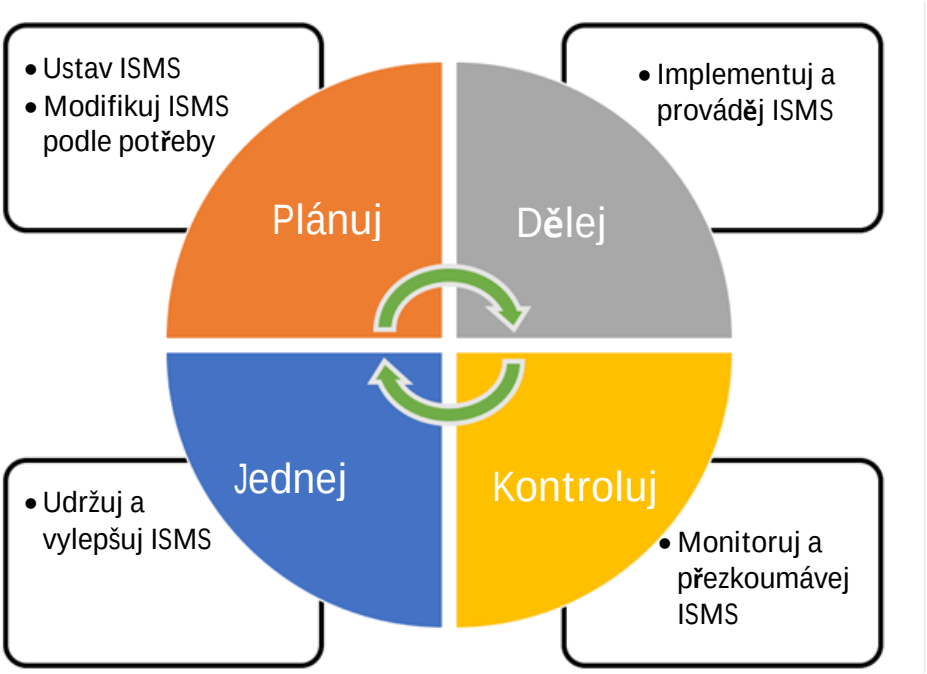
Výše uvedené základní komponenty souvisejí s požadavky tohoto nařízení, pro které obrázek 2 poskytuje zobrazení aspektů na vysoké úrovni, které jsou významnější ve fázi implementace, a těch, které charakterizují provozní fázi, jakož i přezkum a možné zlepšení, pokud funkce nefungují podle plánu.



Obrázek 2: Zobrazení požadavků Části IS z pohledu životního cyklu ISMS

Přístup plánuj-dělej-kontroluj-jednej (PDCA)

PDCA *(Plan-Do-Check-Act)* označuje procesní přístup, který se často používá k vytvoření, implementaci, uplatňování, monitorování, přezkoumávání a zlepšování systémů řízení. Obrázek 3 znázorňuje PDCA aplikovaný na ISMS.



Obrázek 3: Přístup PDCA aplikovaný na ISMS

Přínosy ISMS

Přínosy systému řízení fungujícího v dynamickém, nejistém nebo nepředvídatelném prostředí rizik se v dlouhodobém horizontu projeví pouze tehdy, když organizace zlepší stávající opatření, procesy a řešení na základě posuzování rizik, výkonnosti a vyspělosti, jakož i poučení z incidentů, auditů, neshod a jejich kořenových příčin. Úspěšné přijetí a nasazení ISMS umožňuje subjektu:

— dosáhnout větší jistoty pro management a zainteresované strany, že jejich informační aktiva jsou neustále přiměřeně chráněna proti hrozbám;

— zvýšit svou důvěryhodnost a hodnověrnost poskytnutím důvěry zainteresovaným stranám, že rizika v oblasti bezpečnosti informací s dopadem na bezpečnost letectví jsou náležitě řízena;

— zvýšit odolnost klíčových procesů subjektu proti neoprávněným elektronickým interakcím a zachovat schopnost subjektu rozhodovat a jednat;

— podporovat včasné odhalování mezer v opatřeních, zranitelností nebo nedostatků s cílem předcházet incidentům v oblasti informační bezpečnosti nebo alespoň minimalizovat jejich dopad;

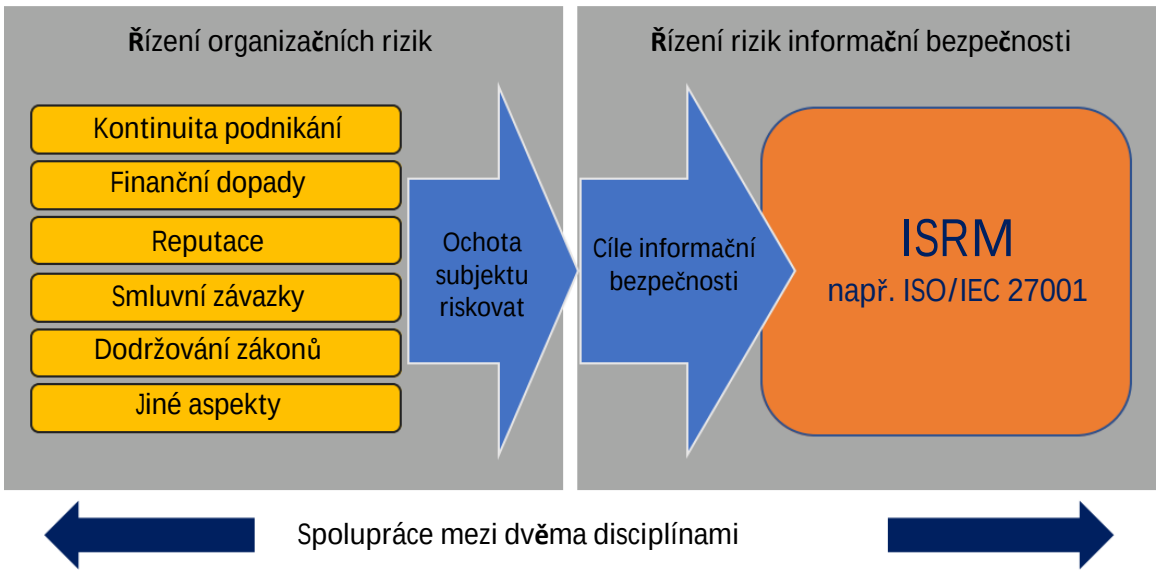
— detekovat a včas reagovat na změny v prostředí subjektu, včetně architektury systému a prostředí hrozeb nebo přijetí nových technologií;

— poskytnout základ pro efektivní a účinnou implementaci komplexní strategie v oblasti informační bezpečnosti v době digitální transformace, rostoucí interkonektivity systémů, vznikajících hrozeb v oblasti informační bezpečnosti a nových technologií.

Vztak k normě ISO/IEC 27001

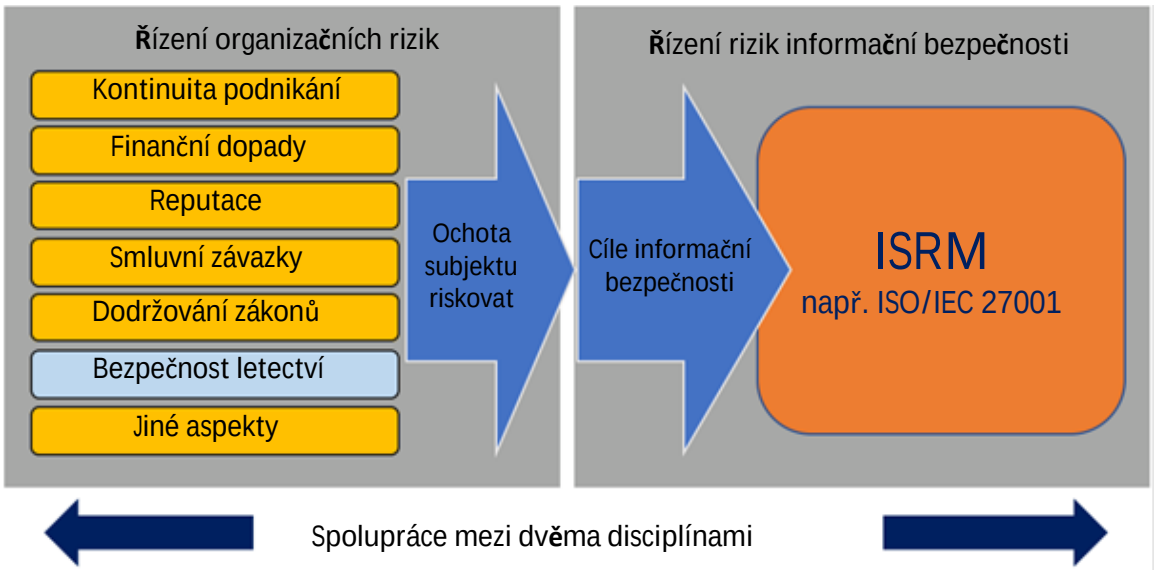
Mezinárodní norma ISO/IEC 27001 je široce přijímaná norma pro ISMS, která specifikuje obecné požadavky na ustavení, implementaci, udržování a neustálé zlepšování ISMS. Zahrnuje také požadavky na posuzování a řešení rizik informační bezpečnosti. Požadavky se vztahují na všechny subjekty bez ohledu na typ, velikost nebo povahu. Shoda ISMS s normou ISO/IEC 27001 může být certifikována akreditovaným certifikačním orgánem. ISO/IEC 27001 je kompatibilní s jinými normami systému řízení (kvality, bezpečnosti atd.), které také přijaly strukturu a termíny definované v příloze Annex SL to ISO/IEC Directives, Part 1, Consolidated ISO Supplement. Tato kompatibilita umožňuje subjektu provozovat jeden systém řízení, který splňuje požadavky více standardů systému řízení.

ISO/IEC 27001 umožňuje subjektům definovat vlastní rozsah auditu a vlastní ochotu organizace riskovat. To zase vede k požadavkům na bezpečnost informací, které poskytují ISMS kritéria přijatelnosti rizik informační bezpečnosti v souladu s ochotou subjektu riskovat (viz obrázek 4).



Obrázek 4: Vztah mezi ochotou subjektu riskovat a cíli informační bezpečnosti

Požadavky na ISMS specifikované tímto nařízením jsou ve většině částí konzistentní a v souladu s ISO/IEC 27001; toto nařízení však zavádí ustanovení specifická v kontextu bezpečnosti letectví. Pokud ISMS založený na ISO/IEC 27001 již subjekt provozuje pro jiný rozsah a kontext, lze jej upravit a rozšířit na oblast působnosti a kontextu tohoto nařízení jednoduchým způsobem na základě analýzy rozsahu a nedostatků. Aby bylo možné získat kredit z certifikací ISO/IEC 27001 za účelem dosažení souladu s Částí IS, musí být bezpečnost letectví zahrnuta do řízení rizik organizace s příslušnou úrovní přijatelnosti rizik stanovenou příslušným předpisem (viz obrázek 5). Proto je nutné pečlivé stanovení rozsahu ISMS v souvislosti s riziky v obůasti bezpečnosti letectví, protože se může lišit od rozsahu ve spojitosti s ostatními organizačními riziky. Aby bylo možné prokázat shodu s nařízením (EU) 2022/1645, může být nutné pečlivé vymezení aspektů ISMS v souvislosti s riziky v oblasti bezpečnosti letectví a dalšími organizačními riziky. To by mohlo mít vliv na rozhodnutí o integraci ISMS.



Obrázek 5: Začlenění aspektů bezpečnosti letectví do ochoty subjektu riskovat

ČÁST IS versus ISO/IEC 27001 – tabulka křížových odkazů

Mapu vztahů mezi hlavními úkoly požadovanými podle Části IS a články a souvisejícími prostředky řízení v ISO/IEC 27001 naleznete v Dodatku II.

AMC1 IS.D.OR.200(a)(1) Systém řízení bezpečnosti informací

Organizace by měla definovat a zdokumentovat rozsah ISMS stanovením činností, procesů, podpůrných systémů a určením těch, které mohou mít dopad na bezpečnost letectví.

Politika bezpečnosti informací by měla být schválena odpovědným vedoucím nebo v případě projekčních organizací – vedoucím projekční organizace, a přezkoumávána v plánovaných intervalech, nebo pokud dojde k významným změnám. Kromě toho by politika měla zahrnovat alespoň následující aspekty s potenciálním dopadem na bezpečnost letectví:

(a) zavázat se dodržovat platnou legislativu, zvážit příslušné normy a osvědčené postupy;

(b) stanovit cíle a výkonnostní opatření pro řízení informační bezpečnosti;

(c) definovat obecné zásady, činnosti, procesy pro organizaci za účelem náležitého zabezpečení systémů a dat informačních a komunikačních technologií;

(d) zavázat se aplikovat požadavky ISMS do procesů organizace;

(e) zavázat se neustále se zlepšovat směrem k vyšším úrovním vyspělosti procesu zabezpečení informací podle IS.D.OR.260;

(f) zavázat se plnit platné požadavky týkající se informační bezpečnosti a jejího proaktivního a systematického řízení a poskytovat odpovídající zdroje pro jeho implementaci a fungování;

(g) určit informační bezpečnost jako jednu ze základních povinností všech manažerů;

(h) zavázat se pravidelně nebo po modifikacích podporovat politiku bezpečnosti informací prostřednictvím školení nebo osvětových setkání pro všechny zaměstnance v rámci organizace;

(i) podporovat zavádění kultury „spravedlivého posuzování *(just culture)*“ a hlášení zranitelností, podezřelých/anomálních událostí a/nebo incidentů v oblasti bezpečnosti informací;

(j) zavázat se sdělit politiku bezpečnosti informací podle potřeby všem relevantním stranám.

Poznámka: Významná změna je výrazná změna nebo modifikace, která má významný dopad na fungování organizace, jako je strukturální změna v rámci organizace v důsledku reorganizací, změna ve firemních procesech (např. práce z domova, používání osobních zařízení), technologický vývoj (např. distribuované výpočetní zdroje, umělá inteligence/strojové učení) nebo vývoj v oblasti hrozeb.

GM1 IS.D.OR.200(a)(1) Systém řízení bezpečnosti informací (ISMS)

POLITIKA A CÍLE V OBLASTI BEZPEČNOSTI INFORMACÍ

Politika bezpečnosti informací by měla vyhovovat účelu příslušného úřadu a řídit jeho vlastní činnosti v oblasti bezpečnosti informací. Taková politika by měla obsahovat potřeby bezpečnosti informací v kontextu dané organizace, prohlášení na vysoké úrovni o směru a záměru činností v oblasti bezpečnosti informací, zásady a nejdůležitější strategické a taktické cíle, kterých má být prostřednictvím ISMS dosaženo, a také obecné cíle informační bezpečnosti nebo specifikace rámce (kdo, jak) pro stanovení cílů informační bezpečnosti. Politika informační bezpečnosti by také měla obsahovat popis stanoveného ISMS, včetně rolí, odpovědností a odkazů na politiky a standardy specifické pro dané téma.

Cíle informační bezpečnosti by měly být:

— konzistentní a v souladu s politikou informační bezpečnosti a měly by brát v úvahu použitelné požadavky na informační bezpečnost, odvozené od zastřešujících cílů organizace, a výsledky

z posuzování a řešení rizik (což naopak podporuje implementaci strategických cílů organizace a politiky informační bezpečnosti);

— pravidelně přezkoumávány, aby bylo zajištěno, že jsou aktuální a stále vhodné;

— měřitelné, pokud je to možné (aby bylo možné určit, zda byl cíl splněn), měly by být SMART (konkrétní *(specific)*, měřitelné *(measurable)*, dosažitelné *(attainable)*, realistické *(realistic)*, časově ukotvené *(timely)*) a spojeny se všemi dotčenými odpovědnými osobami.

Při definování cílů informační bezpečnosti, např. na základě zastřešujících cílů organizace, požadavků na bezpečnost informací nebo výsledků posuzování rizik, by se mělo určit, jak bude těchto cílů dosaženo. Do jaké míry je cílů informační bezpečnosti dosaženo, musí být měřitelné. Pokud je to možné, měla by být měřena pomocí klíčových ukazatelů výkonnosti (KPI), které byly definovány předem (viz zdroje, jako je COBIT 5 pro informační bezpečnost). Doporučuje se začít s definicí omezeného počtu cílů informační bezpečnosti, které jsou pro daný subjekt relevantní, mají spíše dlouhodobý charakter a jsou měřitelné s vynaložením přiměřeného úsilí ve vztahu k dosaženým přínosům.

AMC1 IS.D.OR.200(a)(12)Systém řízení bezpečnosti informací (ISMS)

SLEDOVÁNÍ SHODY

Při zjišťování shody s ustanoveními podle bodů IS.D.OR.200(a)(12) by měla organizace zavést funkci pro pravidelné sledování shody systému řízení s příslušnými požadavky a přiměřenosti postupů, včetně zřízení procesu interního auditu a procesu řízení rizik v oblasti bezpečnosti informací. Pokud již organizace zavedla funkci sledování shody podle prováděcího nařízení pro svou doménu, měla by tato funkce zahrnovat sledování systému řízení s příslušnými požadavky v rámci rozsahu jejích činností. Sledování shody by mělo zahrnovat mechanismus zpětné vazby k nálezům auditu odpovědnému vedoucímu nebo v případě projekčních organizací – vedoucímu projekční organizace, nebo delegovaným osobám, aby se zajistilo provedení nápravných opatření, pokud je to nutné.

GM1 IS.D.OR.200(a)(12) Systém řízení bezpečnosti informací (ISMS)

SLEDOVÁNÍ SHODY

Pro účely sledování shody by měly být prováděny interní audity v plánovaných intervalech, aby se vedení ujistilo o stavu ISMS a poskytly informace o následujícím:

— souladu ISMS s požadavky tohoto nařízení a vlastními požadavky organizace buď uvedenými v politice, postupech a smlouvách v oblasti bezpečnosti informací nebo odvozených z cílů informační bezpečnosti nebo výsledků procesu řešení rizik;

— efektivní implementaci a udržování ISMS.

Interní audity by se měly řídit nezávislým přístupem a rozhodovacím procesem založeným na důkazech. Kromě toho by při sestavování programu auditu měla být zvážena důležitost příslušných procesů a definice kritérií a rozsahu auditu. Měly by být uchovávány zdokumentované informace dokládající výsledky auditu, jejich hlášení příslušnému vedení a program auditu.

AMC1 IS.D.OR.200(a)(13)Systém řízení bezpečnosti informací (ISMS)

Při zjišťování shody s ustanoveními podle bodu IS.D.OR.200(a)(13) by měla organizace zavést a udržovat opatření v oblasti bezpečnosti informací, která jsou dostatečně robustní a účinná, aby chránila informace a zajistila zásadu „potřeba vědět“ (tj. omezení přístupu k informacím pouze na ty, kteří je potřebují k plnění svých povinností). Měl by chránit zdroj informací v souladu s příslušnými ustanoveními stanovenými v nařízení (EU) 2018/1139. Měl by být také v souladu s nařízením (EU) č. 376/2014.

AMC1 IS.D.OR.200(c) Systém řízení bezpečnosti informací (ISMS)

Při zjišťování shody s ustanoveními bodu IS.D.OR.200(c) by organizace měla:

(a) poskytnout přehled struktury konkrétního personálu v oblasti bezpečnosti informací (interního a externího), včetně jejich rolí a odpovědností. Tento přehled bude použit pro řízení a udržování prvků zahrnutých v rozsahu ISMS a bude schválen odpovědným vedoucím nebo v případě projekčních organizací – vedoucím projekční organizace. Organizace by měla přezkoumat přehled struktury v plánovaných intervalech, nebo pokud dojde k významným změnám (viz poznámka v AMC1 IS.D.OR.200(a)(1));

(b) identifikovat a kategorizovat všechny relevantní smluvní organizace používané k implementaci ISMS. Organizace by měla definovat a zdokumentovat postupy pro správu rozhraní a koordinaci mezi touto organozací a jinými organizacemi, včetně smluvních organizací;

(c) identifikovat a definovat všechny klíčové procesy a postupy a systémy interních a externích hlášení, které budou použity k udržení souladu s cíli tohoto nařízení po dobu životního cyklu ISMS. Organizace může upravit stávající procesy nebo postupy pro vyhovění;

(d) identifikovat a zdokumentovat jakékoli další informace, které budou použity k udržení shody s cíli tohoto nařízení;

(e) při vytváření a aktualizaci dokumentovaných informací zajistit vhodnou identifikaci a popis (např. název, datum, autor nebo referenční číslo), jakož i přezkoumání a schválení vhodnosti a přiměřenosti;

(f) kontrolovat dokumentované informace požadované ISMS, aby bylo zajištěno, že jsou:

(1) dostupné a vhodné pro použití tam, kde a kdy jsou potřeba;

(2) adekvátně chráněny (např. proti ztrátěu důvěrnosti, nesprávnému použití nebo ztrátě integrity).

GM1 IS.D.OR.200(c) Systém řízení bezpečnosti informací (ISMS)

Množství informací, které by měly být zdokumentovány, aby byla zachována shoda s cíli tohoto nařízení, se může mezi organizacemi lišit v důsledku různých faktorů, jako je velikost a složitost nebo potřeba harmonizace s jinými již zavedenými procesy řízení. Jako obecné vodítko, s přihlédnutím k dokumentům požadovaným pro vyhovění bodu IS.D.OR.200(a), požadavkům na vedení záznamů uvedeným v IS.D.OR.245 a požadavků na příručku pro řízení bezpečnosti informací uvedených v IS.D.OR.250, je níže uveden neúplný výčet informací, které by měly být zdokumentovány:

(a) politika informační bezpečnosti informací, která by měla zahrnovat cíle organizace v oblasti bezpečnosti informací – viz IS.D.OR.200(a)(1);

(b) zodpovědnosti *(responsibility* – kdo je odpovědný za vykonání svěřeného úkolu*)* a odpovědnosti *(accountablity* – kdo je odpovědný za celý úkol, je odpovědný za to, co je vykonáno*)* pro role související s bezpečností informací – viz IS.D.OR.250(a)(2), (3), (6) a (7) a požadavky na personál uvedené v bodech IS.D.OR.240(a), (b), (c), (d) a (f) a související AMC a GM;

(c) rozsah ISMS a rozhraní s jinými stranami a závislosti na nich – viz IS.D.OR.200(a)(2) a požadavky na bezpečnost informací uvedené v bodech IS.D.OR.205 (a) a (b);

(d) proces řízení rizik v oblasti bezpečnosti informací – viz požadavky na bezpečnost informací uvedené v bodech IS.D.OR.205 a IS.D.OR.210;

(e) archiv rizik identifikovaných v posouzení rizik v oblasti bezpečnosti informací spolu se souvisejícími opatřeními pro řešení rizik (často označovaný jako „registr rizik“ nebo „kniha rizik“) – viz IS.D.OR.245;

(f) důkaz o způsobilosti (kompetencích) nezbytné pro personál vykonávající činnosti požadované tímto nařízením – viz IS.D.OR.240(g) a související AMC a GM;

(g) důkaz o aktuálnosti způsobilosti (kompetencích) personálu vykonávajícího činnosti požadované tímto nařízením – viz IS.D.OR.245(b)(1);

(h) (klíčové) ukazatele výkonnosti odvozené z důkazů o monitorování a měření procesů ISMS.

GM1 IS.D.OR.200(d) Systém řízení bezpečnosti informací (ISMS)

PROPORCIONALITA PŘI IMPLEMENTACI ISMS

Při zavádění procesů a postupů a také při stanovování rolí a odpovědností požadovaných podle bodu IS.D.OR.200(d) by měla organizace především zvážit rizika, která může představovat pro jiné organizace, a také své vlastní vystavení riziku. Mezi další aspekty, které mohou být relevantní, patří potřeby a cíle organizace, požadavky na bezpečnost informací, jeho vlastní procesy a velikost, složitost a struktura organizace, které se mohou v průběhu času měnit.

IMPLEMENTACE ISMS S PODPOROU

V kontextu Části IS iniciují všechny organizace implementaci ISMS určením jeho rozsahu, který je zase založen alespoň na posouzení dopadů na bezpečnost letectví, pro které jsou incidenty týkající se bezpečnosti informací příčinou nebo přispívajícím faktorem. Organizace, bez ohledu na svou velikost, nemusí mít ještě dostatečné znalosti o svých rizicích informační bezpečnosti a mohou zvážit, zda vyhledají podporu u poskytovatele služeb, který může také poskytnout další personál a odborné znalosti během této implementační fáze ISMS. Totéž může platit pro pozdější fáze implementace ISMS a za tímto účelem mohou organizace chtít zvážit ustanovení IS.D.OR.235 a související AMC. Outsourcing specifických funkcí ISMS, jako je monitorování bezpečnosti informací nebo reakce na incidenty poskytovatelům služeb, může pomoci zajistit, aby organizace měla přístup ke zkušeným pracovníkům a odborným znalostem. Podobně mohou organizace chtít, aby je poskytovatel služeb podporoval při provádění posuzování rizik.

Pokud jde o ustanovení vhodného personálu pro zavádění a dodržování ustanovení tohoto nařízení, organizace by se měly vždy odvolávat na AMC1 IS.D.OR.240(f) a GM1 IS.D.OR.240(f) s tím, že více odpovědností může být přiděleno jedné osobě, přičemž je vždy zajištěna nezávislost sledování shody.

Jako úvod k povaze rizik bezpečnosti informací a jejich řízení mohou organizace jako prvotní vodítko použít meziagenturní zprávu NIST Interagency Report (NISTIR 7621 Rev. 1) *„Small Business Information Security: The Fundamentals“*.

ZAČLENĚNÍ ISMS PODLE TOHOTO NAŘÍZENÍ DO STÁVAJÍCÍCH SYSTÉMŮ ŘÍZENÍ

Organizace může při implementaci ISMS využít výhod stávajících systémů řízení tím, že jej integruje do těchto stávajících systémů.

Integrací ISMS do stávajících systémů řízení může organizace snížit úsilí a náklady potřebné k zavedení a udržování ISMS a zároveň zajistit konzistenci a soulad s celkovým přístupem organizace k řízení. Níže je uveden neúplný seznam potenciálních synergií, které lze využít při integraci ISMS do stávajícího systému řízení:

— Využít stávajících zásad a postupů: organizace může použít své stávající zásady a postupy jako základ pro svůj ISMS. To může pomoci zajistit konzistenci a minimalizovat potřebu další dokumentace.

— Sladit ISMS s jinými systémy řízení: organizace může sladit ISMS s jinými systémy řízení, jako jsou systémy řízení bezpečnosti (SMS), aby zajistil, že ISMS bude v souladu s celkovým přístupem organizace k řízení.

— Použít stávající procesy řízení rizik: organizace může použít své stávající procesy řízení rizik k identifikaci a posouzení rizik v oblasti bezpečnosti informací, která mohou vést k rizikům bezpečnosti letectví.

— Znovu použít existující kontroly/opatření: organizace může znovu použít stávající opatření, jako jsou kontroly přístupu nebo proces řízení incidentů, k implementaci opatření v oblasti bezpečnosti informací požadovaných ISMS.

— Proces neustálého zlepšování: organizace může využívat proces neustálého zlepšování stávajících systémů řízení ke zlepšení ISMS v průběhu času.

AMC1 IS.D.OR.200(e) Systém řízení bezpečnosti informací (ISMS)

VÝJIMKA

Aby požádaly příslušný úřad o schválení výjimky podle bodu IS.D.OR.200(e), měly by se organizace řídit pokyny uvedenými v AMC1 IS.D.OR.205(a) a AMC1 IS.D.OR.205(b) k provedení zdokumentovaného posouzení rizik bezpečnosti informací. Aby se opodstatnily důvody pro výjimku, očekává se, že posouzení rizik poskytne vysvětlení pro vyloučení všech prvků z oblasti působnosti ISMS. Je na úřadu, aby určil, zda je toto posouzení pro udělení výjimky považováno za dostatečné.

Organizace, které by chtěly, aby posouzení rizik provedla třetí strana, by měly zvážit požadavky IS.D.OR.235 a související AMC.

GM1 IS.D.OR.200(e) Systém řízení bezpečnosti informací (ISMS)

Jakákoli organizace, která se domnívá, že nepředstavuje žádné riziko pro bezpečnost informací s potenciálním dopadem na bezpečnost letectví, ať už pro ni samotnou nebo pro jiné organizace, může zvážit, že u příslušného úřadu požádá o schválení výjimky podle postupu popsaného v AMC1 IS.D.OR.200(e).

Příkladem organizací, které mohou zvažovat žádost o výjimku, mohou být držitelé DOA nebo POA, kteří navrhují nebo vyrábějí pouze letadlové celky nebo části, které se buď nepodílejí na zajištění strukturální integrity letadla (např. koberce, interiéry) nebo neplní v letadle žádnou významnou funkci související s bezpečností, což zahrnuje, mimo jiné, součásti softwaru letadla, navigace, avioniky, motorů, řízení letu, přistávacího zařízení, hydraulických, elektrických, pneumatických a komunikačních systémů atd. ku, elektřiny, vzduchu, komunikace atd.

Výše uvedený příklad je pouze orientačním potenciálním scénářem, který by mohl poskytnout prvotní základ pro přípravu posouzení rizik bezpečnosti informací, které opodstatňuje vyloučení všech prvků organizace z působnosti ISMS.

GM1 IS.D.OR.205 Posouzení rizik bezpečnosti informací

Část IS nevyžaduje použití žádného specifického rámce zabezpečení informací, jako je ISO, NIST nebo jiné, k vypracování posouzení rizik nebo obecně k implementaci řízení rizik. Každý rámec nabízí různé výhody a žádný z těchto rámců není pro jednotlivou organiizaci dokonalý a měl by být přizpůsoben a upraven tak, aby splňoval celkové potřeby organizace, jakož i konkrétní potřebu zohlednit aspekty bezpečnosti letectví.

Organizace, jejíž rámce bezpečnosti informací získaly průmyslovou certifikaci, může tyto informace poskytnout jako podpůrné artefakty; tyto organizace by však měly prokázat použitelnost průmyslové certifikace na oblast působnosti tohoto nařízení (viz GM1 IS.D.OR.200).

Obecné pokyny pro řízení rizik, včetně posuzování rizik, lze nalézt v ISO/IEC 27005 a ISO/IEC 31000 a také v NIST SP 800-30. Organizace v letectví mohou také zvážit pokyny specifické pro letectví, jak jsou definovány v kapitole řízení rizik v nejnovější verzi EUROCAE ED-201A a podle vhodnosti pro konkrétní provozní prostředí v kapitolách EUROCAE ED-204A, EUROCAE ED-205A a EUROCAE ED-206 pokrývajících řízení rizik.

AMC1 IS.D.OR.205(a) Posouzení rizik bezpečnosti informací

Při provádění posouzení rizik v oblasti bezpečnosti informací by měla organizace zajistit, aby byly identifikovány všechny příslušné prvky bezpečnosti letectví a zahrnuty do rozsahu ISMS podle IS.D.OR.200 a souvisejících AMC.

Způsob, jak vyhovět požadavku v bodě IS.D.OR.205(a), je provést předběžné posouzení rizik na vysoké úrovni nebo posouzení dopadů, provedené v souladu s dokumentovanou metodikou a podle přesných kritérií pro zahrnutí a vyloučení z rozsahu ISMS prvků uvedených v IS.D.OR.205(a).

GM1 IS.D.OR.205(a) Posouzení rizik bezpečnosti informací

IDENTIFIKACE ROZSAHU A HRANIC

Organizace by měla jasně a komplexně porozumět svým činnostem a službám v oblasti letectví, souvisejícím procesům a s tím spojeným informačním systémům a příslušným datovým tokům a výměnám informací, které definují rozsah ISMS a hranice pro posouzení rizik. Organizace by proto měla vypracovat odpovídající dokumentaci o zdrojích a závislostech souvisejících s výpočetní technikou, sítí a smluvními službami, které mají potenciál ovlivnit informační bezpečnost a bezpečnost funkcí, služeb nebo schopností v rámci posouzení rizik.

Následující neúplný seznam uvádí příklady položek, které lze vzít v úvahu pro identifikaci výše uvedeného rozsahu a hranic. Úroveň podrobnosti analýzy může být iterativní proces, s úsilím úměrným očekávané úrovni rizika. Jak je uvedeno výše, účelem je získat znalosti o všech relevantních aktivech, zdrojích a závislostech, které jsou přímou součástí funkcí, služeb a schopností, prostřednictvím následujících činností:

(a) Identifikace provozních vstupů a výstupů relevantních pro funkce, služby a schopnosti organizace; mohou souviset s:

— interními nebo externími zdroji;

— interními nebo externími pronajímanými nebo spravovanými službami nebo jinými závislostmi;

(b) Identifikace všech příslušných aktiv (tj. hardwaru, softwaru, sítě a výpočetních zdrojů) používaných k vytváření, zpracování, přenosu, ukládání nebo přijímání výše uvedených provozních vstupů a výstupů;

(c) Identifikace provozních prostředí (např. kancelář, veřejný prostor, místnost s kontrolovaným přístupem atd.) a umístění všech relevantních aktiv;

(d) U každého aktiva zahrnutého v rozsahu identifikace konkrétních metod, procesů a zdrojů, které budou použity ke správě, provozu a údržbě každého aktiva během jeho životního cyklu, včetně:

— interních nebo smluvních zdrojů;

— smluvních společností vzdáleně spravujících aktiva (tj. poskytovatele spravovaných služeb).

AMC1 IS.D.OR.205(b) Posouzení rizik bezpečnosti informací

Organizace by měla v rámci posouzení rizik bezpečnosti informací určit rozhraní, která má s jinými stranami, jako jsou poskytovatelé služeb, dodavatelské řetězce a další třetí strany, na základě výměny dat a informací a aktiv používaných pro tuto výměnu, což by mohlo vést k situaci, kdy rizika informační bezpečnosti v důsledku vzájemného vystavení mohou buď:

— zvýšit rizika pro bezpečnost letectví, kterým čelí ostatní strany; a/nebo

— zvýšit rizika pro bezpečnost letectví, kterým čelí organizace.

GM1 IS.D.OR.205(b) Posouzení rizik bezpečnosti informací

SDÍLENÍ INFORMACÍ O RIZICÍCH

Organizace tvořící rozhraní by si měly navzájem sdílet informace o možném vystavení rizikům informační bezpečnosti, například podle postupu popsaného v EUROCAE ED-201A, Appendix B – B.1,

B.2 a B.3. Účelem této výměny informací je umožnit organizacím vytvořit odpovídající mapování pro služby uvedené v IS.D.OR.205(a), včetně všech informačních a datových toků, s cílem:

(a) ilustrovat (např. prostřednictvím funkčního diagramu) vztahy logických a fyzických cest spojujících různé zúčastněné strany;

(b) jasně identifikovat všechna aktiva (tj. hardware, software, síť a výpočetní zdroje), která budou při výměně použita;

(c) identifikovat všechny funkce, činnosti a procesy, včetně jejich příslušných informací a dat, které budou vytvářeny, přenášeny, zpracovávány, přijímány a ukládány, a spojit je s odpovědnou stranou, která tyto funkce, činnosti a procesy poskytuje nebo vykonává;

(d) určit pro tyto cesty, tvořící tzv. funkční řetězce, roli strany tvořící rozhraní, jako je výrobce, zpracovatel, odesílatel nebo spotřebitel příslušných informací nebo dat;

(e) určit, zda jedna strana tvořící rozhraní působí jako původce nebo příjemce toku přes takovou cestu.

DVĚ KATEGORIE ORGANIZACÍ Z POHLEDU ROZHRANÍ

Existují dvě kategorie organizací tvořících rozhraní: ty, na něž se vztahuje nařízení (EU) 2023/203 nebo nařízení (EU) 2022/1645, a ty, na něž se nevztahuje.

Pokud má daná organizace rozhraní s organizací, na niž se vztahuje nařízení (EU) 2023/203 nebo nařízení (EU) 2022/1645, každý subjekt:

— je odpovědný za identifikaci rozhraní, která má jeho vlastní organizace s jinými organizacemi a která by mohla mít za následek vzájemné vystavení se rizikům bezpečnosti informací. Subjekt může mít prospěch ze sdílení informací o rizicích, protože tato výměna umožňuje přesnější posouzení těchto rizik.

— zůstává odpovědný za řádné řízení rizik informační bezpečnosti v rámci svého vlastního ISMS.

Ve všech ostatních případech je organizace odpovědná za řádné řízení rizik bezpečnosti informací, která mohou vyplynout z jeho vystavení subjektu tvořícímu rozhraní. Tam, kde je třeba tato rizika řešit, má organizace vždy možnost zavést zmírňující opatření a kontroly v rámci svých vlastních hranic. Ve zvláštním případě, kdy je subjektem tvořícím rozhraní dodavatel, může organizace rozhodnout o řízení rizik prostřednictvím smluvních ujednání a požadovat, aby dodavatel zavedl zmírňující opatření a kontroly v rámci své vlastní organizace.

GM2 IS.D.OR.205(b) Posouzení rizik bezpečnosti informací

PŘÍKLADY LETECKÝCH SLUŽEB

Příklady leteckých služeb, které lze vzít v úvahu při určování rozsahu a rozhraní ISMS, jsou uvedeny v Dodatku III.

AMC1 IS.D.OR.205(c) Posouzení rizik bezpečnosti informací

Organizace by měla používat rámec řízení rizik, který zahrnuje metodiku pro přiřazování rizik k úrovni rizika a stanovení kritérií pro určení přijatelnosti rizik nebo dalšího řešení.

Organizace by měla poskytnout zdokumentované důkazy o posouzení rizik, která mají potenciální dopad na bezpečnost letectví, včetně úrovně rizik. Organizace by měla spojit každé riziko s příslušnými prvky a rozhraními uvedenými v IS.D.OR.205 (a) a (b) a zdokumentovat, zda je riziko přijatelné nebo vyžaduje další řešení.

Organizace by měla poskytnout záruku, že proces posuzování rizik je prováděn s nezbytnou pečlivostí a kázní, a to dokumentací procesu a jeho robustnosti. Přitom by měla organizace zvážit:

(a) reprodukovatelnost a výsledků posouzení v případě podobných vstupů;

(b) opakovatelnost posouzení v čase takovým způsobem, že výsledky různých předchozích posouzení lze porovnat a určit změny;

(c) shromažďování vstupů, které jsou relevantní a platné, zejména:

(1) informace, které umožňují určit důsledky pro bezpečnost;

(2) informace, které umožňují určit potenciál výskytu scénáře hrozby;

(d) iterativní zdokonalování v průběhu času umožňující zpřístupnění detailnějších scénářů hrozeb jako vstupů s cílem snížit nejistotu ohledně hrozeb, zranitelnosti, účelnosti stávajících kontrol/opatření a závislostí na externích subjektech, a to zejména:

(1) zdokonalování počátečních scénářů hrozeb na vysoké úrovni s většími podrobnostmi a specifičností, jak se shromažďuje více dat;

(2) zpřesňování údajů o známých zranitelnostech průběžnou aktualizací informací o jejich zneužitelnosti a souvisejících důsledcích;

(3) přezkoumávání účelnosti stávajících kontrol/opatření a zvážení nově dostupných kontrol/opatření;

(4) upřesnění chápání závislostí na externích subjektech a jejich důsledků pro rizikový profil organizace.

GM1 IS.D.OR.205(c) Posouzení rizik bezpečnosti informací

POSOUZENÍ RIZIK

Mohou být použity níže uvedené úrovně klasifikace rizik pro potenciální výskyt scénáře hrozby a závažnost bezpečnostních důsledků; to však nebrání organizaci ve vytvoření dalších přechodných kategorií, pokud to považuje za nezbytné pro posouzení rizik. Organizace by měla specifikovat a zdokumentovat použité úrovně klasifikace specifické pro organizaci s přesnou kvalitativní nebo kvantitativní definicí, pokud jde o rozsah nebo interval číselných hodnot, aby umožnil dostatečně kalibrovaný, konzistentní odhad, hodnocení a komunikaci v rámci organizace nebo se subjekty tvořícími rozhraní. Potenciál výskytu scénáře hrozby lze vyjádřit jako interval pravděpodobností včetně doby trvání pozorování. Podpůrnou dokumentaci a metody lze nalézt v EUROCAE ED-203A, kapitola 3.6, která odkazuje na vyhodnocení potenciálu výskytu scénáře hrozby v posouzení bezpečnostních rizik EUROCAE ED-202A.

Poznámka 1: Výraz „trvání pozorování“ se vztahuje k časovému období, během kterého je scénář hrozby pozorován nebo monitorován. Je zásadní při určování pravděpodobnosti naplnění scénáře hrozby, protože pravděpodobnost výskytu se může lišit v závislosti na délce sledovaného období.

Poznámka 2: EUROCAE ED-202A a EUROCAE ED-203A byly původně vypracovány pro posuzování rizik bezpečnosti informací v letadlech, ale obecné principy vytvořené v těchto dokumentech mohou být přizpůsobeny jiným rámcům, pokud to organizace považuje za užitečné.

Aby se usnadnila vzájemná srovnatelnost metodik posuzování rizik mezi organizacemi tvořícími rozhraní, může organizace přiřadit posouzení potenciálu výskytu scénáře hrozby k jedné z následujících kategorií:

— Vysoký potenciál výskytu: scénář hrozby pravděpodobně nastane. Útok související se scénářem hrozby je proveditelný a podobné scénáře hrozby se v minulosti vyskytly mnohokrát.

— Střední potenciál výskytu: scénář hrozby pravděpodobně nenastane. Útok související se scénářem hrozby je možný a k podobnému scénáři hrozby mohlo v minulosti dojít.

— Nízký potenciál výskytu: scénář hrozby je velmi nepravděpodobný. Naplnění scénáře hrozby je teoreticky možné; není však známo, že k němu došlo.

Hodnocení potenciálu výskytu scénáře hrozby může být založeno na následujících aspektech:

Ochrana (jak je definováno v EUROCAE ED-203A)

— Bezpečnostní opatření a architektura, které odmítají přístup k aktivům: míra, do jaké je aktivum otevřené přístupu z kompromitovaných systémů

— Přístup k bezpečnostním opatřením: míra, do jaké bezpečnostní opatření brání přístupu/útoku na sebe z kompromitovaných systémů

— Selhání mechanismu: míra, do jaké známá implementace bezpečnostního opatření selže při zabránění útoku

— Detekční metody nebo postupy pro rozpoznání útoku a vhodnou reakci, aby se snížila možnost výskytu scénáře hrozby

Snížení expozice (jak je definováno v EUROCAE ED-203A)

— Podmínky, za kterých může uživatel nebo útočník použít externí přístupové připojení

— Omezení funkčnosti externího přístupového připojení

— Organizační zásady, které kontrolují dobu proveditelnosti pro vývoj nástrojů útoku specifických pro daný produkt

— Management (správa) zranitelností včetně zpravodajské činnosti, skenování, řešení a opakovaného testování zaměřených na odhalení, detekci a řešení hlášených nebo zjištěných zranitelností rychlým způsobem s ohledem na prioritu rizika při vysoké jistotě, aby se omezila plocha, kudy se dá provést útok

— Snížení závažnosti úspěšného útoku (tj. prostřednictvím redundantního systému, který může zachovat kontinuitu služby v případě odepření služby systému kritického pro bezpečnost letectví)

Pokus o útok (jak je definováno v EUROCAE ED-203A)

— Schopnost útočníků, která je určována zdroji a odbornými znalostmi potřebnými k jejich útoku

Schopnost útočníků lze posoudit prostřednictvím několika způsobů, například:

— informací týmů CERT *(computer emergency response teams)* / CSIRT *(computer security incident response teams)*, středisek pro sdílení a analýzu informací (ISAC);

— analýz minulých aktivit, taktik, technik a postupů (TTP) a úspěšnosti útoků.

Ze stejného důvodu může organizace přiřadit výsledek hodnocení závažnosti bezpečnostních důsledků k jedné z následujících kategorií:

— Vysoká závažnost: ty scénáře, které mohou okamžitě nebo se zpožděním způsobit nebo přispět k nebezpečnému stavu, kdy nebezpečný stav znamená událost spojenou s provozem letadla, při které:

  — je osoba smrtelně nebo vážně zraněna;

  — letadlo utrpělo poškození nebo konstrukčnímu selhání;

  — letadlo je buď nezvěstné, nebo je zcela nedostupné;

— Střední závažnost: ty scénáře, které mohou okamžitě nebo se zpožděním způsobit bezpečnostní incidenty nebo k nim přispět, kdy incident znamená jakoukoli jinou událost než nehodu spojenou s provozem letadla, která ovlivňuje nebo by mohla ovlivnit bezpečnost provozu;

— Nízká závažnost: ty scénáře, které mohou okamžitě nebo se zpožděním způsobit nebo přispět k zanedbatelným bezpečnostním následkům.

Příklady vysoké, střední a nízké závažnosti lze pro produkty, systémy ATM a vzdušný prostor nalézt v EUROCAE ED-201A, Appendix B.

Pokud organizace nemůže určit vliv na bezpečnost, posouzení by mělo určit předpoklady z informací o sdílení rizik na rozhraních s jinými organizacemi ve funkčním řetězci, což vede k vlivu na bezpečnost.

Některé z těchto předpokladů lze zajistit certifikací produktů: tam, kde aktiva podléhají certifikaci produktu podle jiných leteckých předpisů týkajících se bezpečnosti informací o produktu, může organizace provádějící posouzení rizik považovat perimetr certifikace produktu za již pokrytý. To by

mělo být přijatelné za podmínky, že tato certifikace je platná a že organizace implementovala pokyny poskytnuté výrobcem OEM pro zachování platnosti certifikace.

Další informace lze nalézt také v nařízení (EU) 2015/1018 o povinném hlášení událostí. Další příklady klasifikace závažnosti dopadů pro oblasti letectví lze nalézt v EUROCAE ED-201A, Appendix B – tabulky B-5, B-6 a B-7.

Kritéria přijatelnosti rizik

Kritéria přijatelnosti rizik jsou kritická a měla by být vyvíjena, specifikována a zdokumentována. Kritéria mohou definovat více prahových hodnot s požadovanou cílovou úrovní rizika, ale umožňují také odpovědnému vedoucímu nebo v případě projekčních organizací – vedoucímu projekční organizace, nebo delegovaným osobám přijmout rizika nad touto úrovní za definovaných okolností a podmínek.

Aby se usnadnila vzájemná srovnatelnost posuzování rizik mezi subjekty tvořícími rozhraní, měla by organizace klasifikovat rizika do následujících kategorií:

— riziko nepřijatelné;

— riziko podmínečně přijatelné;

— riziko přijatelné.

Pokud jde o podmínečnou přijatelnost rizik, kritéria pro přijatelnost by měla brát v úvahu, jak dlouho se očekává, že riziko bude existovat (dočasná nebo krátkodobá aktivita nebo expozice), nebo mohou zahrnovat požadavky na závazek budoucích řešení ke snížení rizika na přijatelnou úroveň v rámci definované doby trvání a ukazují, jak bude riziko řízeno v průběhu času prostřednictvím procesů řízení rizik organizace.

Rizika by navíc měla být podmínečně přijata pouze za podmínky, že organizace prokáže existenci komplexní struktury řízení rizik, která zahrnuje procesy posuzování rizik, řešení rizik a monitorování rizik pro provozy/operace. Řízení rizik by mělo vzít v úvahu variabilitu a konzistenci pravděpodobnosti hrozby, zranitelnosti, stávající kontroly/opatření, externí závislosti a dopad na bezpečnost. Toho se obvykle dosáhne, když organizace dosáhne vyšší úrovně vyspělosti, která je reprezentativní pro funkčnost a opakovatelnost řízení rizik v oblasti bezpečnosti informací – viz GM1 IS.D.OR.260(a).

Následující Obrázek 1 znázorňuje matici přijatelnosti rizik založenou na výše uvedených kategoriích, kterou mohou používat organizace tvořící rozhraní pro vzájemnou srovnatelnost.

ICAO Annex 13 >	Zanedbatelný vliv	Incident	Nehoda
Potenciál výskytu scénáře hrozby	**Nízké bezpečnostní důsledky**	**Mírné bezpečnostní důsledky**	**Vysoké bezpečnostní důsledky**
Vysoký	Podmínečně přijatelné	Nepřijatelné	Nepřijatelné
Střední	Přijatelné	Podmínečně přijatelné	Nepřijatelné
Nízký	Přijatelné	Přijatelné	Podmínečně přijatelné*

Obrázek 1: Příklad matice přijatelnosti rizik pro srovnávací účely

* Potenciál výskytu scénáře hrozby je včas přehodnocen (viz IS.D.OR.205(d)) a monitorován, aby bylo zajištěno, že zůstane nízký a že pokud se riziko naplní, bude včas odhaleno a řešeno.

Komplexní struktura řízení rizik obvykle zahrnuje následující aspekty a procesy:

— opakovatelné a reprodukovatelné posouzení rizik. Jsou-li rizikové faktory považovány za značně nejisté a v nějakém širokém rozmezí hodnot nebo nejsou-li dostatečně přesné,

provedou se další iterace posouzení rizik zahrnující dodatečně shromážděné nebo podrobné informace a podrobnější posouzení, aby se snížila nejistota a zvýšila přesnost;

— důkladný přezkum těchto rizik navržených jako podmíněně přijatelná, který provede odpovědný vedoucí nebo v případě projekčních organizací – vedoucí projekční organizace, nebo delegovaná osoba (osoby), která (který) může uložit další podmínky pro zachování rizik, včetně opatření pro řešení rizik a časového harmonogramu jeho provedení;

— striktní monitorování klíčových ukazatelů rizik, které zahrnuje definovanou a spolehlivou detekci možného vývoje materializace rizik;

— je zaveden systém reakce na incidenty s reaktivními opatřeními, která jsou spouštěna detekčními mechanismy, aby se okamžitě zamezilo důsledkům, zejména u rizikových scénářů s vysokou úrovní závažnosti.

Poznámka: Jak je podrobně popsáno v NIST SP-800 Rev.1, opakovatelnost se týká schopnosti opakovat posouzení v budoucnu způsobem, který je konzistentní a tedy srovnatelný s předchozími posouzeními – což organizaci umožňuje identifikovat trendy. Proto lze proces posouzení rizik klasifikovat jako „opakovatelný“, pokud za podobných podmínek subjekt nebo osoba poskytuje konzistentní výsledky.

Jak je podrobně popsáno v NIST SP-800 Rev.1, reprodukovatelnost se týká schopnosti různých odborníků produkovat stejné výsledky ze stejných dat. Proces posouzení rizik lze proto klasifikovat jako „reprodukovatelný“, když jiný subjekt nebo osoba může při stejných vstupech, předpokladech, kontextu bezpečnosti informací a prostředí hrozeb replikovat stejné kroky a dospět ke stejným závěrům.

Identifikace scénáře hrozby

Scénář hrozby je jedním z možných způsobů, jak by se hrozba mohla zhmotnit. Scénář hrozby obvykle popisuje potenciální útok zaměřený na jednu nebo více zranitelných míst aktiv, stejně jako procesů.

Účelem identifikace scénáře hrozby podle tohoto nařízení je vypracovat seznam scénářů, které mohou vést k ohrožení bezpečnosti informací s dopadem na bezpečnost letectví.

Scénář hrozby je obecně charakterizován následujícím:

— zdroj hrozby útoku na bezpečnost informací;

— vektor útoku a cesta přes organizaci až k aktivu;

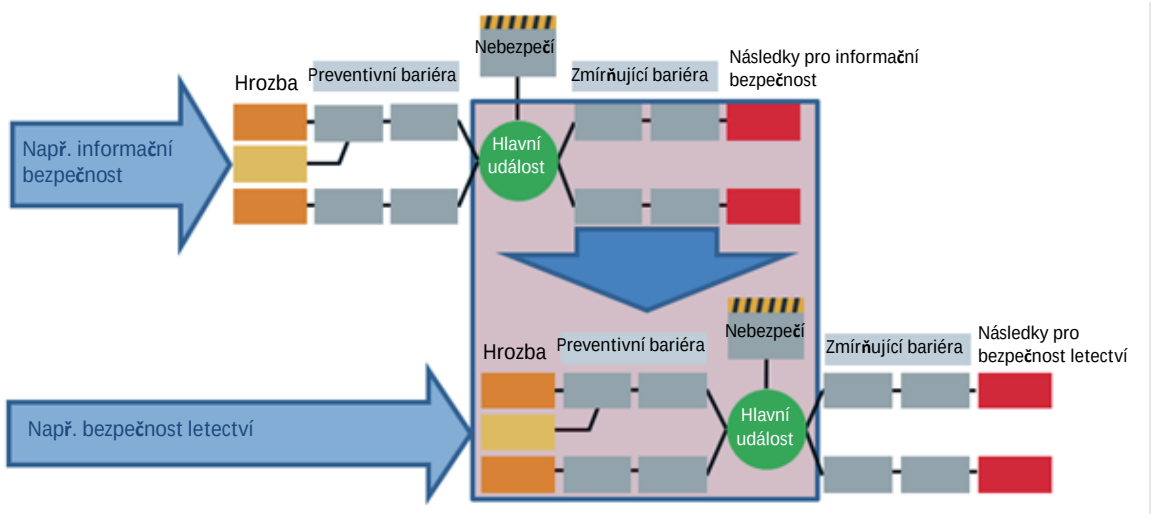
— kontroly/opatření bezpečnosti informací, které by zmírnily útok;

— důsledek útoku včetně dotčených bezpečnostních aspektů.

Pokyny pro identifikaci scénáře hrozeb lze nalézt v EUROCAE ED-202A, kapitola 3.4. Toto není jediný zdroj, kde lze nalézt pokyny, a organizace se může odvolávat na jiné pokyny, které jsou pro jejich použití vhodnější.

Další metody k identifikaci relevantních scénářů hrozeb

Při provádění této analýzy by měly být v průběhu procesu koordinovány aspekty bezpečnosti informací a bezpečnosti, aby bylo zajištěno vzájemné porozumění aplikovaným preventivním opatřením a opatřením ke zmírnění hrozeb. Na následujícím 0brázku 2 jsou interakce mezi bezpečností informací a bezpečností letectví znázorněny prostřednictvím „motýlkového“ diagramu, který zdůrazňuje vazby mezi kontrolami rizik a základním systémem řízení.



Obrázek 2: Interakce mezi oblastmi řízení rizik bezpečností informací a bezpečnosti letectví

Poznámka: Preventivní bariéra nebo opatření je proaktivní akce nebo kontrola implementovaná za účelem snížení pravděpodobnosti naplnění rizika, nebezpečí nebo hrozby, zatímco zmírňující opatření je akce nebo kontrola navržená ke snížení závažnosti nebo dopadu nežádoucí události, pokud by k ní došlo.

Příklady scénářů hrozeb

Katalogy hrozeb mohou poskytnout návod a prvky pro vypracování scénářů hrozeb, které jsou pro organizaci relevantní. Odkazy lze nalézt v ARINC 811 – Att. 3 – Tabulky 3-7 a 3-8 pro příklady katalogů hrozeb a další příklady katalogu hrozeb, jak je poskytují instituce EU – například taxonomie hrozeb ENISA. Toto však není vyčerpávající seznam příkladů, a proto by se identifikace scénářů hrozeb neměla omezovat pouze na tyto příklady. Kromě toho by měly být konzultovány další relevantní zdroje obsahující informace o hrozbách pro bezpečnost informací a o prostředí hrozeb pro bezpečnost informací, aby se příslušnými vstupy podpořil proces posuzování rizik.

Soubor příkladů scénářů hrozeb lze nalézt v Dodatku I.

AMC1 IS.D.OR.205(d) Posouzení rizik bezpečnosti informací

Organizace by měla při zjišťování souladu s cíli uvedenými v bodě IS.D.OR.205(d) vzít v úvahu následující kritéria:

(a) Posouzení rizik provedené podle bodů IS.D.OR.205 (a), (b) a (c) by mělo být v pravidelných intervalech přezkoumáváno, aby se identifikovaly a zohlednily příslušné změny. Periodicitu, s jakou musí být potenciální změny vyhodnoceny, by měla určit organizace provádějící posouzení s ohledem na kritičnost aktiv v rámci posouzení rizik, úrovně zbytkového rizika aktiv v rámci posouzení rizik a jakékoli smluvní nebo regulační požadavky. Vyšší kritičnost nebo úroveň rizika bude vyžadovat častější přezkoumání.

(b) Periodicita přezkumů posouzení rizik by měla být organizací zdokumentována a měla by zahrnovat zdůvodnění, datum schválení a informace o vlastníkovi rizika.

GM1 IS.D.OR.205(d) Posouzení rizik bezpečnosti informací

Kritéria, která je třeba zvážit pro četnost přezkumu posouzení rizik, může být úroveň rizika a také kritičnost a složitost příslušných aktiv. Cílem revize posouzení rizik je spustit přehodnocení rizik, jejich pravděpodobnosti a dopadu v případě relevantních změn. Jedním z možných způsobů je mít víceúrovňový přístup k posouzení rizik, přičemž pro identifikaci změn se používá posouzení rizik na vyšší úrovni. Posouzení rizik na vyšší úrovni by mohlo umožnit identifikaci podrobných rizik, která by

měla být přezkoumána v dalším kroku. Posouzení rizik by měla podléhat pravidelným přezkumům s cílem:

(a) umožnit neustálé zlepšování kvality posouzení rizik;

(b) zajistit efektivnost a účelnost kontrol rizik a zmírňujících opatření jak prostřednictvím jejich návrhu i provozu;

(c) přezkoumat plány a činnosti pro řešení rizik;

(d) identifikovat jakoukoli organizační změnu, která může vyžadovat přezkoumání priorit i řešení rizik;

(e) udržovat přehled o kompletním obrazu rizik; a

(f) identifikovat všechna vznikající rizika.

Přezkoumání posouzení rizik by mělo zahrnovat vlastníky rizik, projektové týmy a případně další zúčastněné strany. Důkaz o přezkoumání posouzení rizik by měl být zdokumentován a měl by zahrnovat:

— doklad o schválení přezkumu určeným vlastníkem rizika; a

— zdůvodnění nebo podklad pro schválení přezkoumání vlastníkem rizika.

Takový důkaz může zahrnovat, ale neomezuje se na:

— zprávy, které představují formu dokumentace pro sledování rizik bezpečnosti informací, která mohou mít dopad na organizaci;

— dokumentaci posouzení rizik bezpečnosti informací;

— výpisy z registru obchodních nebo bezpečnostních rizik.

Periodicita přezkumů posouzení rizik by měla být organizací rovněž dokumentována v příručkách, procesech nebo postupech týkajících se bezpečnosti informací a měla by být v souladu s širšími činnostmi řízení změn a přezkumy řízení bezpečnosti informací. Další pokyny ke kritériím a četnosti přezkumu posouzení rizik lze nalézt v EUROCAE ED-201A, Chapter 4, a také v EUROCAE ED-205A, Chapter 3.2 (pro ATMS/ANS).

GM2 IS.D.OR.205(d) Posouzení rizik bezpečnosti informací

Níže jsou uvedeny příklady změn, které by měly být identifikovány během přezkumu posouzení rizik, protože mohou vyvolat aktualizaci posouzení rizik:

(a) došlo ke změně prvků podléhajících rizikům bezpečnosti informací, jak je uvedeno v IS.D.OR.205(a); změna prvků bude zahrnovat:

— doplnění nebo vyjmutí z rozsahu posouzení rizik jednotlivých prvků;

— změny návrhu nebo konfigurace prvků v rámci rozsahu posouzení rizik, které mají potenciál změnit výsledky posouzení rizik; nebo

— změny hodnot prvků v rozsahu posouzení rizik, které by potenciálně vyvolaly změny úrovní dopadů;

(b) došlo ke změně v rozhraních mezi danou organizací a dalšími organizacemi, s nimiž daná organizace sdílí rizika pro bezpečnost informací nebo na které se spoléhá při zmírňování rizik informační bezpečnosti (např. dodavatelské řetězce, poskytovatelé služeb, poskytovatelé cloudu a zákazníci), jak je uvedeno v IS.D.OR. 205(b), nebo mezi systémem v rozsahu posouzení rizik a jakýmikoli jinými propojenými systémy nebo v rizicích oznámených dané organizaci jinými organizacemi, jak je uvedeno v IS.D.OR.205(b), nebo vlastníky nebo manažery dalších systémů včetně:

— vytvoření nových rozhraní;

— odstranění stávajících rozhraní;

— změny stávajících rozhraní, které by mohly změnit výsledky posouzení rizik.

Poznámka: Některá organizační nebo systémová propojení mohou být s organizacemi, které nespadají do oblasti působnosti tohoto nařízení, jak je definováno v článku 2, a proto nepodléhají požadavkům Části IS. V takovém případě by tyto organizace měly být informovány o své odpovědnosti hlásit výše uvedené změny prostřednictvím smluvních ujednání a požadavků na hlášení mezi dotčenými organizacemi případ od případu a kde je to použitelné;

(c) došlo ke změně informací nebo znalostí používaných pro identifikaci, analýzu a klasifikaci rizik, včetně:

— změn hrozeb a jejich hodnot nebo přidání nových hrozeb, které dříve nebyly posouzeny;

— změn zranitelností nebo přidání nových zranitelností, které nebyly dříve posouzeny;

— změn dopadů nebo následků posuzovaných hrozeb nebo zranitelností;

— změn v agregaci rizik, které mohou vést k nepřijatelným úrovním rizik;

— změn nebo zlepšení v procesu řízení rizik, přístupu k posuzování rizik a souvisejících činnostech;

— změn nebo zlepšení v řešení rizik;

— změn v kritériích používaných k určení přijatelnosti a řešení rizik;

(d) existují ponaučení z analýzy incidentů v oblasti bezpečnosti informací, včetně:

— pochopení, proč a jak k incidentům došlo; a

— přezkoumání všech typů incidentů, včetně incidentů způsobených vnějšími faktory, technickými důvody nebo lidskými chybami (neúmyslné chování). U lidských úmyslných činů lze rozlišovat mezi maligními a benigními činy.

GM1 IS.D.OR.210 Řešení rizik bezpečnosti informací

Nepřijatelná rizika identifikovaná v souladu s bodem IS.~~I~~D.OR.205 vyžadují proces řešení rizik, který může vést k zavedení opatření pro bezpečnost informací, často označovaných jako kontroly bezpečnosti informací.

Pro každé identifikované riziko by organizace měla definovat konkrétní opatření, metody nebo zdroje pro řešení rizika, které budou během životního cyklu každého aktiva použity k:

— řízení snižování rizik;

— monitorování a udržování každého aktiva;

— aktualizaci a plnění činností pro správu konfigurace;

— řízení dodavatelského řetězce;

— řízení smluvních služeb nebo poskytovatele služeb.

Přezkoumání opatření k řešení rizik by mělo zahrnovat úvahy o životním cyklu, které zavádí zařízení, postupy a personál.

Plán řešení rizik jako výsledek procesu řízení rizik by měl zahrnovat stanovení priority rizik, odpovídající informace o cílech a způsobech řešení rizik, aby bylo dosaženo přijatelné úrovně rizika, a také dohodnuté časové harmonogramy specifikující, do kdy by měli odpovědní pracovníci mít provedena opatření k řešení rizik. Časové harmonogramy implementace opatření pro řešení rizik by měl odsouhlasit personál zodpovědný za implementaci a měl by být komunikován s odpovědným vedoucím nebo v případě projekčních organizací – vedoucím projekční organizace, nebo delegovanou osobou (osobami) a jím/jí/jimi akceptován.

Jakékoli následné zpoždění implementace, spolu s jeho příčinou, důvodem, odůvodněním nebo nutností, by mělo být zdokumentováno v plánu řešení rizik pro rizika, která mohou vést k nebezpečnému stavu. Aktualizované řešení rizika by mělo být sděleno příslušnému úřadu v případě, že by materializace

rizika vedla k nebezpečnému stavu. Zpoždění je také podmíněno akceptací odpovědným vedoucím nebo v případě projekčních organizací – vedoucím projekční organizace, nebo delegovanou osobou (osobami). Tato osoba může takovou akceptaci podmínit zavedením nebo dostupností kompenzačních kontrol nebo reaktivních opatření ke sledování, včasné detekci a včasné reakci na materializaci rizika v řešení. Aby bylo možné reagovat včas, může být tým reakce na incident informován, aby zahájil svou připravenost.

Plán řešení rizik může sloužit jako prostředek komunikace s příslušným úřadem k prokázání účinného řešení nepřijatelných rizik. Podobně lze tento plán použít ke komunikaci mezi organizacemi tvořícími rozhraní, jak jsou řízena sdílená rizika.

V souladu s IS.D.OR.205(d) je nezbytný pravidelný nebo podmíněný přezkum posouzení rizik, což zahrnuje přezkum opatření k řešení rizik vypracovaných podle IS.D.OR.210(a) s cílem zjistit, zda jsou stále efektivní nebo vyžadují úpravy.

Kromě toho by organizace měla také zvážit potenciální dopad na účelnost opatření pro řešení rizik tam, kde může vzniknout riziko bezpečnosti sdílených informací v důsledku interakce mezi subjekty tvořícími rozhraní (viz IS.D.OR.235 a související AMC).

AMC1 IS.D.OR.210(a) Řešení rizik bezpečnosti informací

(a) Proces řešení rizik by měl dosáhnout alespoň jednoho z cílů uvedených v IS.D.OR.210(a).

(b) Při zjišťování souladu s cíli podle bodů IS.D.OR.210(a)(1) a IS.D.OR.210(a)(2) by měla organizace vzít v úvahu, že:

(1) opatření vypracovaná podle těchto bodů by měla být prováděna v souladu s plánem řešení rizik s definovanými prioritami založenými na riziku, cíli a dohodnutými časovými harmonogramy a vlastníky.

(2) hlediska životního cyklu by měla být identifikována a asociována, aby byla zajištěna nepřetržitá účelnost opatření pro bezpečnost informací, včetně výměny dat s jinými subjekty;

(3) měla by přezkoumat a aktualizovat posouzení rizik podle IS.D.OR.205(d) s cílem vyhodnotit, zda opatření vyvinutá podle těchto bodů zavádějí nová nepřijatelná rizika nebo pozměňují stávající rizika tak, že se stávají nepřijatelnými.

(c) Řešení rizik by mělo být zdokumentováno a zaznamenáno například v registru rizik, i když bylo riziku zabráněno.

AMC1 IS.D.OR.215(a)&(b) Systém interního hlášení v oblasti bezpečnosti informací

Organizace by měly využívat jako zdroj incidenty zjištěné během činností prováděných k prokázání vyhovění IS.D.OR.220(a). Organizace by měly mít mechanismus pro shromažďování oznámení o událostech od personálu a zdrojů mimo společnost, včetně dodavatelů, partnerů, zákazníků, softwaru s otevřeným zdrojovým kódem a výzkumníků v oblasti bezpečnosti informací. Mechanismus pro shromažďování informací personálem a externími zdroji by měl být snadno dostupný a sdělitelný.

Organizace by měla shromažďovat všechny události shromážděné prostřednictvím detekčních prostředků pro interní analýzu. Každá událost by měla být analyzována, aby se zjistilo, zda je možné ji hlásit, a pokud ano, jaký potenciální nebo skutečný dopad na bezpečnost letectví nastal. Události bezpečnosti informací by měly být zvažovány v kombinaci s jinými událostmi, aby byla zajištěna korelace k identifikaci incidentů nebo zranitelností s potenciálním dopadem na bezpečnost letectví.

Organizace by měla zvážit výsledek posouzení rizik a využitelnost nových zranitelných míst objevených během detekčních činností prováděných podle opatření požadovaných v IS.D.OR.220(a).

Organizace by měla identifikovat všechny interní zainteresované strany, které vyžadují oznámení o konkrétním incidentu nebo zranitelnosti, a zajistit, aby tyto zainteresované strany obdržely všechny

nezbytné informace o incidentu nebo zranitelnosti, aby mohly účinně a včas jednat a podpořit požadované lhůty pro detekování a reakci.

GM1 IS.D.OR.215(a)&(b) Systém interního hlášení v oblasti bezpečnosti informací

VZTAH MEZI INTERNÍM A EXTERNÍM HLÁŠENÍM

Organizace by měly shromažďovat a hlásit interně incidenty a zranitelnosti s cílem pokrýt všechny položky v oblasti působnosti tohoto nařízení. Jak interní, tak externí hlášení jsou nezbytná pro kompletní a efektivní systém hlášení. Interní hlášení by měla být včas posouzenaa tam, kde je potenciální dopad na bezpečnost nebezpečným stavem, by organizace měly iniciovat hlášení těchto interních zpráv podle IS.D.OR.230.

GM2 IS.D.OR.215(a)&(b) Systém interního hlášení v oblasti bezpečnosti informací

ORGANIZACE SBĚRU A HODNOCENÍ UDÁLOSTÍ BEZPEČNOSTI INFORMACÍ

Ve velkých organizacích je běžnou praxí centralizovat operace týkajících se informační bezpečnosti v bezpečnostním operačním centru – SOC *(security operations centre)* a využívat systém správy událostí a informací v oblasti bezpečnosti informací – SIEM *(information security information and event management)*. Systém SIEM shromažďuje všechny události ze zdrojů, jako jsou protokolové soubory log, ve společné databázi a umožňuje analytikům a respondentům ve společném SOC tyto události kontrolovat a jednat podle nich. Organizace se mohou rozhodnout použít SOC pro události související s Částí IS samostatně nebo v kombinaci s událostmi, které nepodléhají Části IS, ale které jsou pro organizaci zajímavé, jako jsou události související s obchodními zájmy. Události lze automaticky agregovat, korelovat a analyzovat, aby bylo možné odhalit abnormální chování vedoucí k incidentům bezpečnosti informací.

Organizace, které nemají schopnost SOC a nepoužívají systém SIEM, musí zvážit, jak zavést procesy, aby splnily požadované schopnosti sběru a vyhodnocování a také lhůty pro detekování a reakce.

GM3 IS.D.OR. 215(a)&(b) Systém interního hlášení v oblasti bezpečnosti informací

RELEVANTNÍ INFORMACE TÝKAJÍCÍ SE INCIDENTŮ A ZRANITELNOSTÍ

Pochopení příčin a faktorů přispívajících k incidentům a zranitelnostem bezpečnosti informací v souvislosti s Částí IS umožňuje získat poučení a vnést nápravu do procesů a návrhu aktiv. Pochopení příčin a přispívajících faktorů však nemusí být vždy možné nebo nemusí napomáhat neustálému zlepšování bezpečnosti letectví. Očekává se, že tam, kde zranitelnost pramení z aktiv vyvinutých výhradně nebo primárně pro letectví, bude možné provést nezbytné zjištění kořenových příčin. Tyto kořenové příčiny poskytnou dotčené organizaci (organizacím) informaci ke zlepšení procesů a návrhu aktiv s cílem napravit zranitelnost a zajistit, aby taková zranitelnost nebyla zavedena do jiných aktiv. Pochopení kořenových příčin zranitelnosti také umožňuje letecké komunitě získat z tohoto ponaučení a vyhnout se tak podobným zranitelnostem v budoucnu.

GM1 IS.D.OR.215(c) Systém interního hlášení v oblasti bezpečnosti informací

Pokud se toto nařízení vztahuje i na smluvní organizace, výměna informací a hlášení by měly být pokryty v rámci řízení sdílených rizik a prostřednictvím uzavření externí dohody mezi organizacemi. Pokyny týkající se vytváření externích dohod lze nalézt v dokumentu EUROCAE ED-201A, Chapter 4.4 *External agreements*.

Obecněji a ve všech ostatních případech by každá smlouva o poskytování služeb měla obsahovat standardní doložky týkající se povinností smluvní organizace:

— hlásit v dohodnuté lhůtě incidenty bezpečnosti informací, které mohou mít dopad na organizaci uzavírající smlouvu (zadavatele). Incidenty a zranitelnosti, které by mohly vést k nebezpečným podmínkám, by měly být hlášeny co nejdříve a takovým způsobem, aby bylo možné zajistit externí ohlašovací povinnost podle IS.D.OR.230;

— určit kontaktní místo (osobu) pro správu (řízení) incidentů a případné krizové řízení.

V některých případech smluvní organizace, jako jsou poskytovatelé služeb s distribuovanými zdroji, nemusí být schopny nabídnout žádná ad hoc hlášení. V těchto případech lze požadavek na vnitřní hlášení splnit jinými prostředky, které splňují cíl tohoto ustanovení. Smluvní organizace mohou například poskytnout aktuální seznam zranitelností ovlivňujících systémy v rámci rozsahu smluvních služeb. Tento seznam by měl být organizací uzavírající smlouvu (zadavatelem) sledován jako součást interního hlášení událostí bezpečnosti informací.

GM1 IS.D.OR.215(d) Systém interního hlášení v oblasti bezpečnosti informací

Spolupráce podle bodu IS.D.OR.215(d) může být doložena sdílením prvků ze záznamů incidentů, které mohou podpořit činnosti v oblasti bezpečnosti informací jiných organizací. V případě, že jsou organizace vázány smluvními závazky, může tato smlouva obsahovat i závazek ke spolupráci. Organizace mohou zvážit vytvoření formálních dohod (např. memoranda o porozumění), které vymezují role a odpovědnosti za spolupráci v oblasti bezpečnosti informací, jako jsou schůzky v oblasti správy, společné aktivity v oblasti vývoje a sdílení indikátorů ohrožení – IoC *(indicator of compromise)* v reálném čase.

Kromě toho lze závazku spolupráce dosáhnout také aktivní účastí organizace na iniciativách pro sdílení informací v oblasti bezpečnosti informací; například centra pro sdílení a analýzu informací – ISAC *(information sharing and analysis center)*. Kromě toho se mohou organizace pro vlastní povědomí přihlásit k odběru upozornění na zranitelnosti a hrozby, jako jsou ty, které distribuují CERT.

GM1 IS.D.OR.220 Incidenty bezpečnosti informací – odhalení, reakce a zotavení

Aniž je dotčena definice „události bezpečnosti informací“ v článku 3 nařízení (EU) 2022/1645, mezi události, které naznačují potenciální materializaci nepřijatelných rizik, patří obě události (tj. cokoli, co způsobuje škodu nebo má potenciál způsobit škodu) a odhalování zranitelností. Ve skutečnosti jsou rizika informační bezpečnosti spojena s potenciálem, že hrozby zneužijí zranitelnosti, proto je odhalení zneužitelné zranitelnosti událostí bezpečnosti informací.

Ve světle tohoto, v kontextu tohoto nařízení:

— činnosti odhalování požadované podle IS.D.OR.220(a) zahrnují zjišťování zranitelností;

— činnosti reakce požadované podle IS.D.OR.220(b) zahrnují řízení zranitelností.

AMC1 IS.D.OR.220(a) Incidenty bezpečnosti informací – odhalení, reakce a zotavení

ODHALOVÁNÍ

Při plnění požadavku v IS.D.OR.220(a) by měla organizace definovat a zavést strategii pro odhalování incidentů v oblasti bezpečnosti informací, které mohou mít potenciální dopad na bezpečnost.

To by mělo být provedeno tak, aby bylo zajištěno, že je strategie odhalování schopna pokrýt přinejmenším všechny známé hrozby bezpečnosti informací pro jejich aktiva, které se mohou zhmotnit v ohrožení bezpečnosti s nepřijatelnými důsledky.

STRATEGIE ODHALOVÁNÍ

Aby mohla organizace určit rozsah odhalování událostí, měla by:

(a) identifikovat seznam scénářů hrozeb z rizik identifikovaných podle IS.D.OR.205;

(b) identifikovat minimálně ta aktiva, která, jsou-li ohrožena, přispívají ke scénáři (scénářům), který se může zhmotnit v nebezpečném stavu. Pro tuto identifikaci aktiv by měla být rovněž zvážena opatření zavedená podle IS.D.OR.210.

Poznámka: Podíl aktiva na scénáři hrozby a naplnění nebezpečného stavu by měl být posouzen také zvážením celého funkčního řetězce. V některých případech může být aktivum na konci funkčního řetězce, a je-li ohroženo, vliv na bezpečnost je přímý a může být okamžitý; naopak, pokud je aktivum daleko od konce funkčního řetězce a je ohroženo, účinek by se měl šířit a může být opožděn.

GM1 IS.D.OR.220(a) Incidenty bezpečnosti informací – odhalení, reakce a zotavení

STRATEGIE ODHALOVÁNÍ

Při vývoji strategie odhalování pro položky v rozsahu odhalování událostí by měla organizace definovat podmínky, které spouštějí proces, který by například vyžadoval zásah personálu a další analýzu. Tyto podmínky u daných položek lze definovat pomocí prvků z:

(a) očekávané funkční základny: zapojit se do identifikace odchylek od očekávaného funkčního provozu systému (s výjimkou funkcí/kontrol pro bezpečnost informací);

(b) očekávané základny informační bezpečnosti: zapojit se do identifikace odchylek od očekávaného fungování informační bezpečnosti kontrol bezpečnosti informací.

Tyto podmínky by měly brát v úvahu jak abnormální chování, tak podstatné odchylky od výchozích hodnot a relevantní korelaci více nezávislých událostí.

Další pokyny k cílům pro stanovení strategie odhalování lze nalézt v EUROCAE ED-206, Chapter 4.

AMC1 IS.D.OR.220(b) Incidenty bezpečnosti informací – odhalení, reakce a zotavení

(a) INCIDENTY

Organizace by měla při zjišťování souladu s cíli uvedenými v bodě IS.D.OR.220(b) ve vztahu k incidentům vzít v úvahu následující aspekty:

(1) Příprava postupů a vymezení rolí a odpovědností pro včasnou, efektivní a řádnou reakci na jakékoli relevantní incidenty bezpečnosti informací.

(2) Postup reakce by měl:

(i) zvážit varování, jednotlivá nebo kombinovaná, z IS.D.OR.220(a)(2), a ve spolupráci s příslušným personálem posoudit jejich potenciální dopady na bezpečnost letectví;

(ii) stanovit v souladu s IS.D.OR.220(b)(2) strategii izolace *(containment)* pro každou kategorii aktiv s ohledem na možný nejhorší možný účinek a omezení mise a poskytne kritéria, která označují, kdy je incident izolován;

(iii) definovat v souladu s IS.D.OR.220(b)(3) přijatelný dopad na bezpečnost a informační bezpečnost každého aktiva v rozsahu, když selžou v důsledku naplnění scénáře hrozby.

(3) Doba reakce by měla být úměrná úrovni dopadu hodnocené v (2)(iii).

(4) Opatření pro reakci prováděná podle IS.D.OR.220(b) by měla vycházet z postupu reakce uvedeného ve výše uvedeném bodě (a)(2) a měla by zohledňovat zejména následující:

(i) maximální přijatelné snížení úrovně bezpečnosti aktiva v rámci rozsahu incidentu;

(ii) akce, jako je rezistence, izolace, klamání a řízení možných způsobů selhání systémů, které přispějí k dosažení přijatelného snížení úrovně bezpečnosti uvedeného v bodě (i) při minimalizaci dopadu na provoz;

(iii) zdroje potřebné k provádění akcí uvedených v bodě (ii).

(5) Doba a opatření reakce by měly zohledňovat potenciální bezprostřední negativní dopad na bezpečnost, pokud je opatření přijato dříve, než bude plně ověřeno, že nezpůsobí další bezprostřední dopady na bezpečnost.

(b) ZRANITELNÁ MÍSTA (ZRANITELNOSTI)

Organizace by měla při zjišťování souladu s cíli uvedenými v bodě IS.D.OR.220(b) ve vztahu ke zranitelnostem vzít v úvahu následující aspekty:

(1) Stanovení strategie řízení zranitelností definující postupy, role a odpovědnosti, aby bylo možné včas, účinně a řádně reagovat na jakékoli zjištěné relevantní zranitelnosti.

(2) Opatření pro reakci prováděná podle bodu IS.D.OR.220(b) by měla být založena na maximálním přijatelném riziku položek v rozsahu zranitelnosti s ohledem na nejhorší možný scénář zneužití zranitelnosti.

(3) Doba reakce by měla být úměrná předtriáži při varováních a posouzení potenciálního dopadu zranitelnosti, pokud je zneužita.

GM1 IS.D.OR.220(b) Incidenty bezpečnosti informací – odhalení, reakce a zotavení

Útok je považován za izolovaný (tj. nešíří se dále), pokud byly identifikovány hranice incidentu a hrozba se za tyto hranice nešíří. Další pokyny lze nalézt v dokumentu EUROCAE ED-206 – Chapter 5.

Termín „varování“, jak je používán v IS.D.OR.220, by měl být chápán jako výstraha, která by vyžadovala včasnou informovanost a reakci týmu pro řízení událostí v oblasti bezpečnosti informací.

V kontextu reakce na bezpečnost informací se „klamání“ týká řady technik, jejichž cílem je uvést v omyl potenciální útočníky nebo uživatele se zlými úmysly, a tím chránit systém a jeho data. Techniky klamání, jako jsou honeypoty nebo drobečková navigace *(breadcrumb trails)*, jsou navrženy tak, aby zmátly, zpomalily nebo odvedly útočníky, zvýšily jejich náklady a riziko a zároveň poskytly obráncům cenný čas a zpravodajské informace.

Poradenský materiál týkající se strategie řízení zranitelnosti lze nalézt v dokumentu EUROCAE ED-206, Chapter 3.4 – *Vulnerability management considerations*. Toto není jediný zdroj, kde lze nalézt návod, a organizace se může odvolávat na jiné poradenské materiály, které jsou pro jejich použití vhodnější.

AMC1 IS.D.OR.220(c) Incidenty bezpečnosti informací – odhalení, reakce a zotavení

Při plnění požadavku v IS.D.OR.220(c) by měla organizace vypracovat postup zotavení se (obnovy) z incidentu zahrnující alespoň následující:

(a) seznam těch aktiv, která umožňují bezpečný provoz, jakož i vzájemné závislosti mezi nimi, tvořící rozsah obnovy;

(b) popis procesu s nezbytnými prioritními akcemi, které mají být provedeny pro návrat aktiv v rozsahu obnovy se do bezpečného a zabezpečeného stavu;

(c) zdroje potřebné k provedení akcí definovaných v bodě (b), aby se zajistilo, že tyto zdroje budou po výskytu incidentu snadno dostupné;

(d) cíle doby obnovy, které by měly být stanoveny ve vztahu ke kritičnosti bezpečnosti aktiv v rozsahu obnovy.

GM1 IS.D.OR.220(b)&(c) Incidenty bezpečnosti informací – odhalení, reakce a zotavení

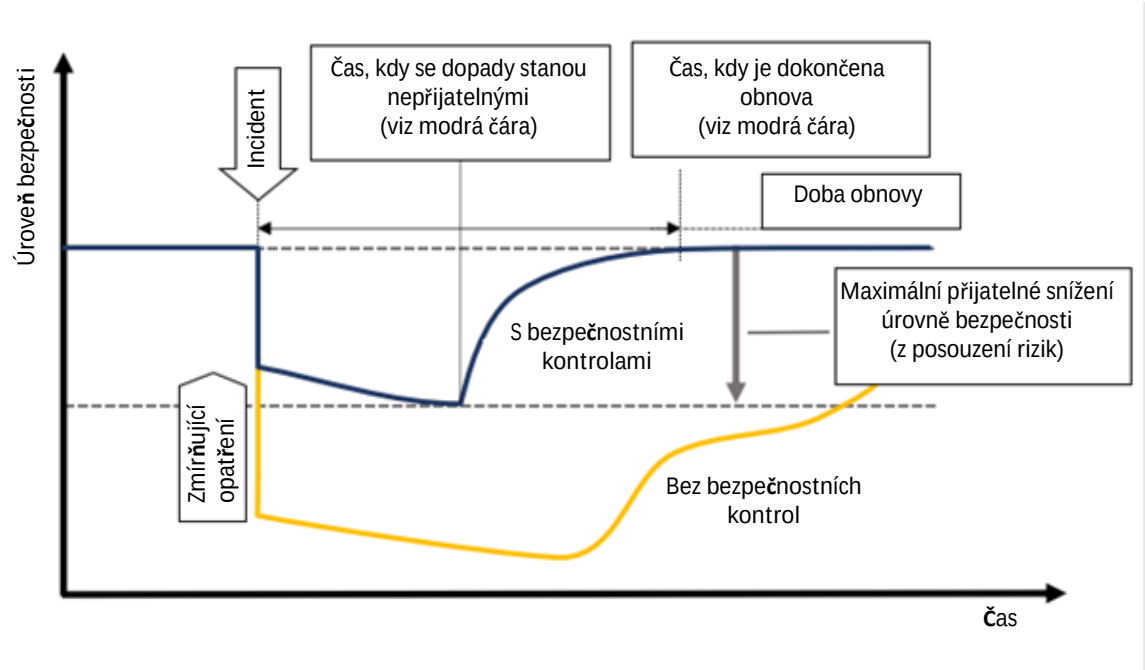
CÍLE A ČASOVÝ ROZVRH OBNOVY

Bod IS.D.OR.220(b) se zabývá podmínkami událostí, které se mohou rozvinout nebo se z nich vyvinuly incidenty bezpečnosti informací, které mohou mít potenciální dopad na bezpečnost letectví, a vyžadují, aby byla zavedena opatření pro reakci a obnovu, s cílem zajistit, že provozní bezpečnost zůstane nad minimální přijatelnou úrovní.

Úroveň provozu a bezpečnosti mohou být vzájemně propojené, takže v některých případech, kdy je úroveň provozu ohrožena incidentem bezpečnosti informací a klesá, úroveň bezpečnosti dělá totéž. To je například případ řízení letového provozu; pokud se letové provozní služby omezí nebo se stanou nespolehlivými, sníží se i bezpečnost letů.

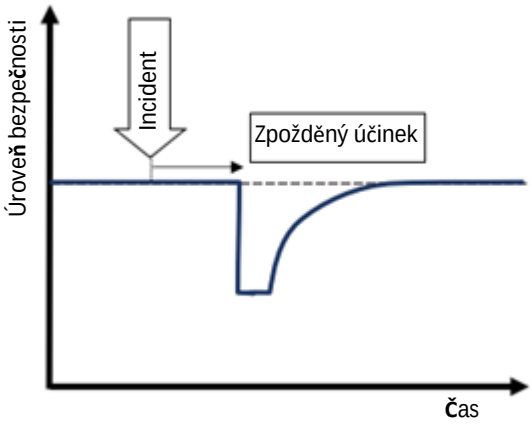
V jiných případech však může být vztah mezi úrovní provozu a bezpečností inverzní, nebo mohou být odděleny, takže když dojde k incidentu a úroveň provozu klesne, úroveň bezpečnosti zůstane zachována. Jedním z příkladů je narušení procesu nahrávání softwaru na palubě letadla. V tomto případě by detekovaný incident následovaný rozhodnutím přerušit operaci nahrávání softwaru zachoval stávající úroveň bezpečnosti.

Následující Obrázek 1 znázorňuje koncepční rámec, který lze vzít v úvahu pro definici cílů reakce a obnovy, včetně doby obnovy. V nejhorším případě představuje, jak se očekávaná úroveň provozní bezpečnosti (úroveň bezpečnosti *(safety level)*) pro proces nebo činnost může měnit v průběhu času, když dojde k incidentu bezpečnosti informací. V tomto scénáři je úroveň bezpečnosti nejprve snížena incidentem, a poté se s plynoucím časem dále snižuje. Obrázek také ukazuje očekávaný účinek, který by měla mít zmírňující opatření a kontroly: v omezení poklesu provozní bezpečnosti, jakmile dojde k incidentu, a ve zlepšení zotavení se (obnovy), tedy návratu na očekávanou úroveň bezpečnosti.

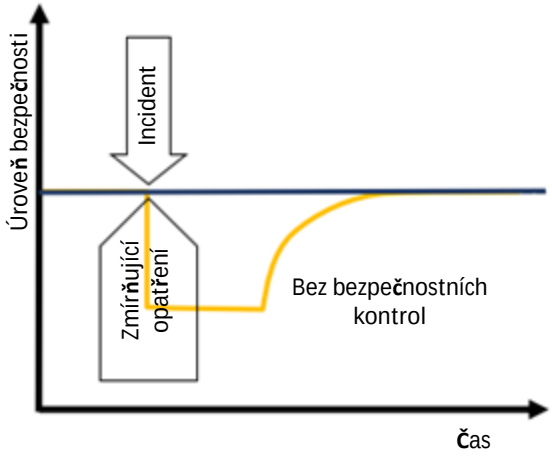


Obrázek 1: Koncepční rámec pro definici cílů reakce a obnovy

Jak již bylo zmíněno, mohou existovat různé vztahy mezi úrovní provozu a bezpečností, které by vedly k odlišnému zobrazení výše uvedeného obrázku. V určitých případech může mít incident zpožděný účinek na úroveň bezpečnosti (např. narušené vývojové prostředí), jak je znázorněno na Obrázku 2, nebo nemusí mít žádný dopad, pokud je řádně kontrolován, jako v případě narušeného procesu nahrávání softwaru uvedeného výše, který je znázorněn na Obrázku 3.



Obrázek 2: Incident se zpožděným účinkem na bezpečnost



Obrázek 3: Incident s plně zmírněným dopadem na bezpečnost

Kromě toho je třeba poznamenat, že mohou existovat různé způsoby, jak lze stejný incident řešit, protože existuje několik faktorů, které mohou ovlivňovat bezpečnost.

V praxi mohou být cíle doby obnovy uvedené v AMC1 IS.D.OR.220(c) vyjádřeny jako seznam zdrojů a služeb, které mají být obnoveny podle pořadí priorit, v rámci rozsahu obnovy. Poradenský materiál týkající se cílů doby obnovy lze nalézt v dokumentu EUROCAE ED-206, Chapter 7.3.5.

GM1 IS.D.OR.220(c) Incidenty bezpečnosti informací – odhalení, reakce a zotavení

Postup zotavení se nebo plán obnovy by měl popisovat činnosti pro zotavení se (obnovu) z incidentu a interní nebo externí zdroje, které jsou dotčeny (např. zaměstnanci, IT, budovy, poskytovatelé). Poradenský materiál týkající se plánu obnovy lze nalézt v dokumentu EUROCAE ED-206, Chapter 7 – *Recover*.

Měly by být k dispozici zdroje potřebné k uplatnění nápravných opatření, aby bylo možné provést nápravná opatření včas poté, co došlo k incidentu. Tyto zdroje mohou být dostupné interně nebo mohou být zajišťovány smluvními organizacemi, jak je stanoveno v IS.D.OR.235. Smlouvy o činnostech obnovy by měly být uzavřeny předtím, než dojde k incidentu (proaktivně), a smlouva by měla obsahovat ujednání, aby smluvní strana mohla včas reagovat.

Návrat do bezpečného a zajištěného stavu může zpočátku vyžadovat nouzová opatření, což jsou činnosti, které jsou zahájeny na základě nejlepších dostupných informací v danou chvíli, než je dosaženo úplného pochopení situace a tato opatření mohou potenciálně snížit úroveň služeb nebo funkcionalit. Návrat do bezpečného a zajištěného stavu by měl být vyhodnocen oproti počátečnímu posouzení rizik a může se pouze dočasně lišit od běžných provozních podmínek. Jakékoli zvýšení zbytkového rizika a trvání tohoto zvýšení rizika, tj. v důsledku provádění mimořádných opatření, by však mělo být zdokumentováno a přijato na správné úrovni odpovědnosti.

Zde uvedené činnosti pro zotavení se (obnovu) mohou být také výsledkem reakce na incidenty, o nichž organizace obdržela informace, že vyžadují provedení odpovídajících opatření, aby reagoval na incidenty nebo zranitelnosti informační bezpečnosti s potenciálním dopadem na bezpečnost letectví.

V takovém kontextu nemusí mít organizace proces nebo plán obnovy pokrývající konkrétní událost. Proto je ze strany organizace obvykle vyžadována definice konkrétního plánu obnovy a jeho schválení příslušným úřadem.

AMC1 IS.D.OR.225 Reakce na nálezy oznámené příslušným úřadem

Vyhovění IS.D.OR.225 by mělo být řízeno tak, jak je pro každou organizaci požadováno v odpovídajícím prováděcím nařízení pro danou oblast, jak je uvedeno v čl. 2 odst. 1 nařízení (EU) 2022/1645, co se týče reakce na nálezy oznámené příslušným úřadem. Nařízení pro danou oblast může vyžadovat, aby organizace reagovala na nálezy podle jejich kategorizace.

GM1 IS.D.OR.225 Reakce na nálezy oznámené příslušným úřadem

Požadavek na kategorizaci nálezů a lhůtu, ve které by měly být provedeny kroky v IS.D.OR.225(a), lze nalézt v odpovídajícím prováděcím nařízení pro danou oblast v rámci požadavků na úřady. Při otevření nálezů v souvislosti s tímto nařízením se příslušný úřad bude řídit výše uvedeným požadavkem.

GM1 IS.D.OR.230 Systém externího hlášení v oblasti bezpečnosti informací

Organizace jsou povinny hlásit události svému příslušnému úřadu.

PŘÍKLADY

Projekční organizace schválené EASA: příslušným úřadem je EASA.

Letečtí provozovatelé osvědčení příslušným úřadem členského státu: příslušným úřadem je příslušný úřad členského státu.

ZVLÁŠTNÍ PŘÍPADY

V situaci, kdy má organizace dvě osvědčení leteckého provozovatele (AOC) ve dvou různých členských státech EU (stát A a B), musí být události týkající se letadel provozovaných pod AOC státu A hlášeny příslušnému úřadu státu A, kdežto události týkající se letadel provozovaných pod AOC státu B musí být hlášeny příslušnému úřadu státu B.

U organizací, které mají více oprávnění, bude hlášení podáno příslušnému úřadu schválené části organizace, kde došlo k incidentu nebo kde byla zjištěna zranitelnost. V případě, že incident/zranitelnost ovlivňuje více oprávnění, bude hlášení provedeno všem příslušným úřadům.

Pro organizace, které jsou držiteli oprávnění, ale působí mimo EU (např. podle Části 145), je příslušným úřadem EASA a musí podávat hlášení Agentuře.

Letadla dvojího užití *(dual-use)* – zranitelnost může být nutné hlásit prostřednictvím vojenského i civilního systému hlášení, pokud má vliv na funkci/systém dvojího užití. Informace hlášené prostřednictvím civilního systému hlášení by měly být sanitizovány (tj. všechny citlivé informace by měly být řádně odstraněny).

AMC1 IS.D.OR.230(a)&(b) Systém externího hlášení v oblasti bezpečnosti informací

Aby organizace vyhověla ustanovením podle IS.ID.OR.230 (a) a (b), měla by hlásit:

(a) jakoukoli událost, na kterou se vztahuje nařízení (EU) č. 376/2014 a která vznikla úmyslně neoprávněnou elektronickou interakcí;

(b) incidenty bezpečnosti informací s potenciálním významným rizikem pro bezpečnost letectví, na které se nevztahuje nařízení (EU) č. 376/2014;

(c) zranitelnosti, které představují významné riziko pro bezpečnost letectví a nejsou dosud adekvátně zmírněny v souladu se schválenou strategií řízení zranitelností (viz AMC1 IS.D.OR.220(b)).

U výše uvedených hlášení je odpovědností příslušných úřadů podle Části IS zajistit soulad s článkem 7 tohoto nařízení a předložit veškeré relevantní informace, které je třeba sdílet s příslušnými orgány pro bezpečnost informací určenými podle článku 8 směrnice (EU) 2016/1148.

GM1 IS.D.OR.230(a)&(b) Systém externího hlášení v oblasti bezpečnosti informací

VZTAH MEZI IS.D.OR.230(b) A NAŘÍZENÍM (EU) č. 376/2014

Nařízení Evropského parlamentu a Rady (EU) č. 376/2014 stanovuje požadavky na hlášení událostí v civilním letectví, analýzu těchto hlášení a navazující opatření. V\hovění s bodu IS.D.OR.230(b) nezbavuje organizace povinnosti dodržovat nařízení (EU) č. 376/2014.

Pro každou kategorii oznamovatelů definuje nařízení (EU) č. 2015/1018 povahu položek, které mají být povinně hlášeny. Nařízení (EU) č. 376/2014 rovněž uvažuje o dobrovolném hlášení dalších položek, které oznamovatel vnímá jako hrozbu pro bezpečnost letectví.

Kromě toho vyhovění nařízení (EU) č. 376/2014 nezbavuje organizace povinnosti vyhovět bodu IS.D.OR.230(b). Nemělo by to však vést ke vzniku dvou paralelních systémů hlášení a bod IS.D.OR.230(b) a nařízení (EU) č. 376/2014 by se v tomto ohledu měly považovat za vzájemně se doplňující.

V praxi to znamená, že povinnosti hlášení podle bodu IS.D.OR.230(b) na jedné straně a povinnosti hlášení podle nařízení (EU) č. 376/2014 na straně druhé jsou slučitelné. Tyto povinnosti hlášení lze plnit pomocí jednoho kanálu hlášení. Kromě toho může každá fyzická nebo právnická osoba, která má více než jednu roli podléhající povinnosti podat hlášení, splnit všechny tyto povinnosti prostřednictvím jediného hlášení. Organizacím se doporučuje, aby to řádně popsaly ve své organizační příručce, aby se zabývaly případy, kdy jsou odpovědnosti vykonávány jménem organizace.

ANALÝZA NAVAZUJÍCÍCH OPATŘENÍ

Pokud analýza události hlášené podle nařízení (EU) č. 376/2014 později zjistí, že kořenovou příčinou události nebo faktorem přispívajícím k události byla úmyslná neoprávněná elektronická interakce, měla by organizace aktualizovat své oznámení příslušnému úřadu.

VÝZNAMNÉ RIZIKO PRO BEZPEČNOST LETECTVÍ

V souladu s definicí události podle čl. 2 odst. 7 nařízení (EU) č. 376/2014 by jakýkoli incident nebo zranitelnost v oblasti bezpečnosti informací, které mohou představovat významné riziko pro bezpečnost letectví, měly být považovány za událost podléhající hlášení. Významným rizikem pro letectví se rozumí nebezpečný stav, tj. stav, který může vést k nehodě nebo vážnému incidentu (jak je definováno v ICAO Annexu 13).

Poznámka: Při posuzování možnosti, že by účinky incidentu bezpečnosti informací mohly vést k nebezpečnému stavu, by organizace měla zvážit kombinaci účinků, pokud incident zahrnuje více systémů; ve skutečnosti mohou být některé předpoklady o nezávislosti systému, které mohou platit pro náhodné události, úmyslnými činy porušeny.

VZTAH MEZI IS.D.OR.230(b)(1) A JINÝMI POŽADAVKY NA HLÁŠENÍ UDALOSTÍ BEZPEČNOSTI INFORMACÍ SOUVISEJÍCÍCH S LETECKÝMI VÝROBKY NEBO ČÁSTMI

U organizací, na které se vztahují požadavky na hlášení událostí v oblasti bezpečnosti informací souvisejících s leteckými výrobky nebo částmi, se za dostatečné k dosažení vyhovění požadavku v bodě IS.D.OR.230(b)(1) považuje vyhovění specifickým ustanovením prováděcího nařízení pro jejich oblast. Například u organizací, na které se vztahuje nařízení (EU) č. 748/2012, lze hlášení provést v souladu s bodem 21.A.3A Přílohy I (Část 21) uvedeného nařízení.

AMC1 IS.D.OR.230(c) Systém externího hlášení v oblasti bezpečnosti informací

V rámci celkové lhůty 72 hodin by míra naléhavosti pro předložení hlášení měla být určena úrovní dopadu na bezpečnost, o kterém se soudí, že je výsledkem incidentu bezpečnosti informací nebo zjištěné zranitelnosti. Pokud osoba, která identifikuje možný nebezpečný stav, usoudí, že událost vedla k bezprostřednímu a zvláště významnému nebezpečí, příslušný úřad očekává, že bude informován okamžitě a nejrychlejšími možnými prostředky (telefon, fax, e-mail, dálnopis atd.) o všech podrobnostech, které jsou v dané chvíli k dispozici.

GM1 IS.D.OR.230(c) Systém externího hlášení v oblasti bezpečnosti informací

Poradenský materiál týkající se hlášení incidentů a zranitelností bezpečnosti informací lze nalézt v dokumentu EUROCAE ED-206, Chapter 6.4.2.2 – *Reporting timeline* a Chapter 6.4.5 – *Reporting information content*. Toto není jediný zdroj, kde lze nalézt pokyny, a organizace se mohou odvolávat na jiné pokyny, které jsou pro jejich použití vhodnější.

Poznámka: Osoba provádějící hlášení události podle nařízení (EU) č. 376/2014 nemusí být schopna určit povahu události. To platí zejména pro bezpečnost informací a tento výsledek může vycházet z forenzní analýzy, která určuje, že daná události má povahu týkající se bezpečnosti informací. Hodnocení bude provedeno jako součást procesu počátečního interního hlášení (viz IS.D.OR.215 a související AMC). Vyhodnocení události může prokázat možnost, že se zhmotní do nebezpečného stavu s přihlédnutím k pravděpodobnosti realizace.

GM1 IS.D.OR.235 Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací

Organizace se mohou rozhodnout, že určité činnosti zadají dodavatelům, a to jak pro své vlastní provozní potřeby, tak za účelem vyhovění tomuto nařízení (činnosti týkající se řízení bezpečnosti informací). Činnosti nasmlouvané pro provozní potřeby mohou spadat do oblasti působnosti Části IS, a proto musí být příslušná rizika v oblasti bezpečnosti informací řízena v souladu s požadavky v bodech IS.D.OR.205 a IS.D.OR.210. Namísto toho podléhají činnosti týkající se řízení bezpečnosti informací zvláštním ustanovením IS.D.OR.235, protože záležitosti týkající se těchto činností mohou mít na organizaci významný dopad.

Proto cíle bodu IS.D.OR.235 jsou:

(a) chránit kritické a citlivé informace a aktiva, když s nimi nakládají organizace smluvně zajišťující poskytování činností týkajících se řízení bezpečnosti informací (včetně organizací v dodavatelském řetězci) buď v jejich zařízeních, nebo v zařízeních dané organizace, nebo když jsou přenášeny mezi danou organizací a smluvními organizacemi nebo k nimž mají smluvní organizace vzdálený přístup;

(b) zabránit zavádění rizik v oblasti bezpečnosti informací prostřednictvím produktů a služeb vyvinutých nebo poskytovaných smluvními organizacemi danou organizací v rámci zajišťování činností týkajících se řízení bezpečnosti informací;

(c) zajistit, že jsou rizika v oblasti informační bezpečnosti řízena ve všech fázích vztahu se smluvními organizacemi.

GM2 IS.D.OR.235 Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací

(a) Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací je způsob, jak alokovat úkoly organizace uzavírající smlouvu (zadavatele) na třetí strany (smluvní organizace

(dodavatele)). Organizace uzavírající smlouvu zůstává zodpovědná *(responsible)* za dozor nad smluvní organizací (organizacemi) a odpovědný *(accountable)* za dodržování tohoto nařízení.

(b) Smlouva může mít formu písemné dohody, schvalovacího dopisu, servisního dopisu, memoranda o porozumění atd., jak je pro dané smluvní činnosti vhodné.

GM3 IS.D.OR.235 Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací

PŘÍKLADY

Následující Tabulka 1 uvádí některé příklady činností týkajících se řízení bezpečnosti informací, které mohou být zajišťovány smluvně ve vztahu k ustanovením uvedeným v IS.D.OR.200.

Tabulka 1: Příklady činností týkajících se řízení bezpečnosti informací, které mohou být zajišťovány smluvně

Body IS.D.OR.200, které se vážou k činnostem	Příklad smluvních činností
(a)(1): zavede politiku v oblasti bezpečnosti informací, která stanoví obecné zásady organizace s ohledem na potenciální dopad rizik bezpečnosti informací na bezpečnost letectví;	Návrh politiky informační bezpečnosti a poradenství
(a)(2): identifikuje a přezkoumává rizika bezpečnosti informací v souladu s bodem IS.D.OR.205;	Identifikují aktivity, zařízení a zdroje. Identifikují rozhraní s jinými organizacemi, která by mohla být vystavena rizikům bezpečnosti informací. Provádí analýzu rizik nebo její část, např. identifikuje a klasifikuje rizika informační bezpečnosti.
(a)(3): definuje a provádí opatření k řešení rizik bezpečnosti informací v souladu s bodem IS.D.OR.210;	Definují, vyvíjejí a implementují opatření. Ověřují počáteční a pokračující účelnost implementovaných opatření (např. cvičení červený tým/ modrý tým, penetrační testování, skenování zranitelnosti atd.). Sdělují zúčastněným stranám výsledek posouzení rizik a jejich odpovědnosti v rámci procesu řešení rizik.
(a)(4): provádí systém interního hlášení v oblasti bezpečnosti informací v souladu s bodem IS.D.OR.215;	Definují, vyvíjejí a implementují systém interního hlášení, který umožní shromažďovat a vyhodnocovat události v oblasti bezpečnosti informací a zranitelnosti zařízení, procesů a služeb.
(a)(5): definuje a provádí v souladu s bodem IS.D.OR.220 opatření potřebná k odhalení událostí bezpečnosti informací, identifikuje takové události, které jsou považovány za incidenty s potenciálním dopadem na bezpečnost letectví, s výjimkou případů povolených bodem IS.D.OR.205(e), a reaguje na tyto incidenty bezpečnosti informací a zotavuje se z nich; (a)(6): provádí opatření, která byla oznámena příslušným úřadem jako okamžitá reakce na	Definují, vyvíjejí a implementují opatření k odhalení událostí. Definují, vyvíjejí a implementují opatření, která budou reagovat na podmínky jakékoli události. Definují, vyvíjí a implementují opatření zaměřená na zotavení se z incidentů bezpečnosti informací. Implementuje opatření okamžité reakce na incident nebo zranitelnost bezpečnosti informací, jak byla oznámena příslušným úřadem.

Body IS.D.OR.200, které se vážou k činnostem	Příklad smluvních činností
incident nebo zranitelnost bezpečnosti informací s dopadem na bezpečnost letectví;	
(a)(7): přijme v souladu s bodem IS.D.OR.225 vhodné opatření k řešení nálezů oznámených příslušným úřadem;	Identifikuji kořenové příčiny. Definují plán nápravných opatření. Poskytují důkaz o implementovaných nápravných opatřeních pro uzavření nálezu.
(a)(8): provádí systém externího hlášení v souladu s bodem IS.D.OR.230 s cílem umožnit příslušnému úřadu přijmout vhodná opatření;	Definují, vyvíjejí a implementují systém externího hlášení, který umožní sdělování informací o incidentech v oblasti bezpečnosti informací a zranitelnosti zařízení, procesů a služeb příslušnému úřadu a v případě potřeby držiteli schválení návrhu nebo organizaci odpovědné za návrh.
(a)(9): splňuje požadavky uvedené v bodě IS.D.OR.235 při uzavírání smluv na jakoukoli část činností uvedených v bodě IS.D.OR.200 s jinými organizacemi;	Nepoužitelné
(a)(10): splňuje požadavky na personál stanovené v bodě IS.D.OR.240;	Činnosti odpovědného vedoucího / vedoucího projekční organizace v rámci ustanovení pro „společnou odpovědnou osobu“, jak je uvedeno v IS.D.OR.240. Sledování shody, jak předpokládá IS.D.OR.240. Smluvní organizace k zajištění, že je k výkonu činností souvisejících s tímto nařízením ve službě dostatek personálu. Definují, vyvíjejí a poskytují adekvátní školení k dosažení kompetencí, které jsou u personálu požadovány. Provádí kontroly před nástupem do zaměstnání.
(a)(11): splňuje požadavky na vedení záznamů stanovené v bodě IS.D.OR.245;	Definují, vyvíjejí a implementují zabezpečenou archivaci. Poskytování zabezpečeného datového centra (jako služby) Poskytování aktualizací záznamů
(a)(12): sleduje soulad organizace s požadavky tohoto nařízení a poskytuje zpětnou vazbu v souvislosti s nálezy odpovědnému vedoucímu / vedoucímu projekční organizace za účelem zajištění účinného provádění nápravných opatření;	Sledování shody (jak předpokládá IS.D.OR.240), včetně provádění nezávislých auditů.
(a)(13): chrání, aniž jsou dotčeny příslušné požadavky na hlášení incidentů, důvěrnost veškerých informací, které organizace případně obdržela od jiných organizací, podle úrovně jejich citlivosti.	Definují, vyvíjejí a implementují řešení na ochranu důvěrnosti jakýchkoli informací.
(b): Aby neustále splňovala požadavky uvedené v článku 1, organizace provádí proces neustálého zlepšování v souladu s bodem IS.D.OR.260.	Provádějí nezávislé hodnocení účelnosti a vyspělosti. Definují, vyvíjejí a implementují nezbytná opatření ke zlepšení.
(c): Organizace v souladu s bodem IS.D.OR.250 dokumentuje všechny klíčové procesy, postupy,	Vypracování dokumentace s podrobnými informacemi o všech klíčových procesech,

Body IS.D.OR.200, které se vážou k činnostem	Příklad smluvních činností
úlohy a povinnosti požadované za účelem dosažení souladu s bodem IS.D.OR.200(a) a zavede proces pro změnu uvedené dokumentace. Změny uvedených procesů, postupů, úloh a povinností se řídí podle bodu IS.D.OR.255.	postupech, rolích a odpovědnostech vyžadovaných pro splnění bodu IS.D.OR.200(a) (např. zásad bezpečnosti informací, obecného popisu personálu, postupů pro specifikaci vyhovění). Definují, vyvíjejí a implementují procesy pro schvalování dodatků a změn.

AMC1 IS.D.OR.235(a) Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací

(a) DOZOR NAD SMLUVNÍ ORGANIZACÍ

Aby mohla daná organizace vykonávat dozor nad smluvní organizací, měla by mít:

(1) proces, který zajistí vyhovění ustanovením v tomto nařízení týkajících se smluvních činností;

(2) strukturovaný proces sledující očekávané plnění smlouvy, který zahrnuje:

(i) vymezení a odsouhlasení rozsahu činností;

(ii) definici rolí a odpovědností stran (tj. organizace uzavírající smlouvu (zadavatele) a smluvní organizace (dodavatele));

(iii) definici a přezkum ukazatelů KPI;

(iv) reakci na odchylku od smluvních závazků;

(v) provádění auditů shody, podle předem definovaného rozsahu a cílů, s cílem vyhodnotit provozní a související zabezpečovací činnosti;

(vi) poskytování zpětné vazby o výsledcích auditů shody jak v rámci dané organizace, tak smluvní organizaci a reakce na nálezy. Zpětná vazba o výsledku auditů shody v rámci organizace uzavírající smlouvu by se měla dostat k odpovědnému vedoucímu nebo v případě projekčních organizací – vedoucímu projekční organizace, nebo delegované osobě (osobám), aby bylo zajištěno řádné sledování reakce na nálezy (tj. provedení nápravných opatření), nebo bude-li to považováno za nutné, ukončení smlouvy.

Poznámka: Právo dané organizace provádět audity shody smluvní organizace by mělo být zahrnuto ve smlouvě mezi těmito stranami.

(b) ŘÍZENÍ RIZIK SPOJENÝCH SE SMLUVNÍMI ČINNOSTMI

Aby mohla řádně řídit rizika spojená se smluvními činnostmi, měla by organizace splňovat tato kritéria:

(1) Před outsourcingem jakýchkoli činností týkajících se řízení bezpečnosti informací se provádí předchozí posouzení dodavatelů. Posouzení by mělo hodnotit kompetence dodavatelů, jejich udržitelnost a kvalifikace ve vztahu k činnostem, které mají být smluvně zajišťovány.

(2) Dochází k posuzování rizik spojených s poskytováním smluvních činností, které bylo dohodnuto mezi danou organizací podle Části IS a smluvní organizací.

(3) Organizace zřizuje a udržuje vhodné komunikační kanály pro bezpečnost informací se smluvní organizací.

GM1 IS.D.OR.235(a) Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací

PŘEDCHOZÍ POSOUZENÍ

Účelem předchozího posouzení je vyhodnotit kompetence, udržitelnost a kvalifikace dodavatelů ve vztahu k činnostem v oblasti bezpečnosti informací, které mají být smluvně zajišťovány. Toto předchozí posouzení může být nutné provést s přihlédnutím k dalším právním požadavkům nebo postupům zadávání zakázek, které se na organizaci vztahují, a může být proto provedeno různými způsoby, jako například:

(a) v případě veřejných nabídek zahrnutí požadavků způsobilosti do zadávací dokumentace pro potenciální dodavatele;

(b) přezkoumání certifikací bezpečnosti informací potenciálním dodavatelům udělených externími a nestrannými auditory;

(c) přezkoumání sebehodnotících dotazníků sestavených potenciálními dodavateli.

POSOUZENÍ RIZIK SPOJENÝCH S POSKYTOVÁNÍM SMLUVNÍCH ČINNOSTÍ

Posouzení rizik by mělo vzít v úvahu úroveň vyspělost smluvní organizace a mělo by vzít v úvahu následující:

(a) identifikaci a posouzení kritických a citlivých informací a aktiv, které mohou být s externími dodavateli sdíleny nebo které mohou být externími dodavateli poskytovány;

(b) identifikaci požadavků dané organizace na bezpečnost informací, které se vztahují na smluvní organizaci;

(c) hodnocení schopnosti smluvní organizace (stávající i nové smluvní organizace) plnit požadavky organizace uzavírající smlouvu (zadavatele) na bezpečnost informací, a to prostřednictvím posouzení dodavatele;

(d) posouzení rizik, které může smluvní organizace přinést.

Toto odsouhlasené posouzení rizik by také mělo vzít v úvahu role a odpovědnosti organizace uzavírající smlouvu (zadavatele) a smluvní organizace (dodavatele) a také jejich rozhraní.

GM2 IS.D.OR.235(a) Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací

AUDIT SMLUVNÍCH ORGANIZACÍ

Při auditování dodavatele, se kterým má uzavřenu smlouvu na provádění činností řízení bezpečnosti informací, by měla organizace vzít v úvahu následující aspekty:

— rozsah auditu, jakož i cíl by měly být omezeny na procesy, zdroje (tj. personál smluvní organizace, systémy/vybavení, sítě) a data používaná k provádění smluvních činností podle Části IS;

— audity shody a/nebo implementace by měly být prováděny podle uvážení organizace uzavírající smlouvu (zadavatele);

— nálezy zjištěné během auditu by měly být řešeny prostřednictvím plánu nápravných opatření spolu s časovým rámcem, které má organizace uzavírající smlouvu (zadavatel) potvrdit.

AMC1 IS.D.OR.235(b) Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací

Aby zajistila na vyžádání přístup příslušného úřadu do smluvní organizace, měla by organizace podle Části IS zajistit, že jsou takový požadavek nebo ustanovení zahrnuty do smluvní dokumentace.

Přístup příslušného úřadu do smluvních organizací by měl být přinejmenším rovnocenný přístupu udělenému organizaci uzavírající smlouvu (zadavateli) a v každém případě by měl být dostatečný k zajištění posouzení trvalého souladu smluvních činností s platnými požadavky.

GM1 IS.D.OR.235(b) Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací

Přístup do smluvní organizace znamená mít možnost vidět důkaz vyhovění smluvních činností (jako jsou artefakty, dokumenty, nezávislé certifikace).

Důkazu vyhovění lze dosáhnout buď předáním dokumentů a/nebo přístupem k informacím v prostorách v souladu s „rozsahem auditu“, jak je definován ve smlouvě.

V těch případech, kdy by organizace využívala komerční běžné služby se standardními smluvními doložkami jako součást nasmlouvaných činností týkajících se řízení bezpečnosti informací, měla by organizace zvážit, zda tyto doložky poskytují dostatečný přístup k požadovaným informacím.

Možnost navštívit prostory by měla být vyhodnocena s ohledem na různé aspekty, jako je citlivost souvisejících informací nebo praktická dostupnost smluvní organizace (např. smluvní organizace je poskytovatel služeb s distribuovanými zdroji).

GM1 IS.D.OR.240 Požadavky na personál

Cíle požadavků obsažených v bodech (a) až (e) jsou:

(a) zajistit, že je zavedena účinná organizační struktura, aby byly splněny požadavky tohoto nařízení;

(b) zajistit důvěru v ostatní organizace, se kterými sdílejí rizika.

AMC1 IS.D.OR.240(a)(2) Požadavky na personál

PODPORA POLITIKY BEZPEČNOSTI INFORMACÍ

Odpovědný vedoucí nebo v případě projekčních organizací – vedoucí projekční organizace dané organizace by se měl ujistit, že politika bezpečnosti informací je zaměstnancům známa a snadno přístupná, a to přiměřeně jejich povinnostem.

AMC1 IS.D.OR.240(a)(3) Požadavky na personál

ZÁKLADNÍ POROZUMĚNÍ NAŘÍZENÍ

Aby bylo možné prokázat základní porozumění tomuto nařízení, odpovědný vedoucí organizace nebo v případě projekčních organizací – vedoucí projekční organizace by měl být schopen vysvětlit zastřešující cíle tohoto nařízení a jeho důsledky pro organizaci.

GM1 IS.D.OR.240(a)(3) Požadavky na personál

ZÁKLADNÍ POROZUMĚNÍ NAŘÍZENÍ

V případě, že odpovědný vedoucí nebo v případě projekčních organizací – vedoucí projekční organizace nemá žádné předchozí zkušenosti v oblastech činností souvisejících s Částí IS, může získat potřebné znalosti tím, že se zúčastní školení zahrnujícího obsah tohoto nařízení a technický základ pro vyhovění (shodu). Školicí materiál by měl zejména pokrývat zastřešující cíle Části IS a hodnocení by mělo posoudit porozumění těmto regulatorním cílům.

AMC1 IS.D.OR.240(b) Požadavky na personál

JMENOVÁNÍ OSOBY NEBO SKUPINY OSOB

Osoba nebo skupina osob jmenovaná podle bodu IS.D.OR.240(b) se zodpovědností *(responsibility)* zajistit vyhovění požadavkům tohoto nařízení by měla představovat řídící strukturu organizace.

Tato osoba nebo skupina osob má přímý přístup k odpovědnému vedoucímu nebo v případě projekčních organizací – k vedoucímu projekční organizace (nebo společné odpovědné osobě, je-li jmenována), aby zajišťovala vedení, směr a podporu plánování, implementaci a fungování procesu a standardů, aby byly v souladu s nařízením. Měli by mít přímý přístup k tomu, aby odpovědného vedoucího nebo v případě projekčních organizací – vedoucího projekční organizace (nebo společnou odpovědnou osobu) řádně informovali o záležitostech shody a bezpečnosti informací (například prostřednictvím setkání organizovaných na pravidelné bázi).

Jmenování by mělo zohledňovat možnost, že osoba nemusí být po určitou dobu schopna plnit jí přidělené organizační úkoly, a tedy také určit potřebné zástupce.

Tyto jmenované osoby by měly prokázat plné porozumění požadavkům tohoto nařízení, aby byly schopny zajistit, že procesy a standardy organizace přesně reflektují použitelné požadavky. Jejich úlohou je zajistit, aby byla shoda proaktivně řízena a aby byly zdokumentovány všechny rané varovné signály neshody a aby se podle toho jednalo.

Popis funkcí a zodpovědností jmenovaných osob a zástupců, včetně jejich jmen, by měl být obsažen v ISMM (viz bod IS.D.OR.250(a)(2)).

GM1 IS.D.OR.240(b) Požadavky na personál

Podmínka dlouhodobé nepřítomnosti jmenované osoby nastává, když tato osoba není schopna plnit svěřené organizační povinnosti. Je-li například požadováno, aby činnost týkající se řízení bezpečnosti informacíí vykonávaly jmenované osoby ve stanoveném intervalu, nepřítomnost se považuje za dlouhodobou, pokud tento interval překročí, a proto může dojít ke zranitelnosti v činnosti řízení.

GM1 IS.D.OR.240(b)&(c) Požadavky na personál

Jmenování lze provést prostřednictvím e-mailu, organizačního schématu, tabulky rolí a zodpovědností atd., které organizace obvykle používá. Organizace může přijmout pro výše uvedené pozice řízení bezpečnosti informací jakékoli názvy, ale měla by příslušnému úřadu identifikovat názvy a osoby vybrané k výkonu těchto funkcí.

GM1 IS.D.OR.240(c) Požadavky na personál

FUNKCE SLEDOVÁNÍ SOULADU (SHODY)

Osoba jmenovaná podle bodu IS.D.OR.240(c) se zodpovědností za řízení funkce sledování souladu (shody) požadované podle bodu IS.D.OR.200(a)(12) může být stejná osoba jako osoba odpovědná za funkci sledování souladu (shody) vyžadovaná prováděcím předpisem pro danou oblast, nebo ji může informovat.

AMC1 IS.D.OR.240(d) Požadavky na personál

KOORDINACE

Kritéria pro zavedení koordinace, která zajistí adekvátní integraci řízení bezpečnosti informací v rámci organizace, jsou následující:

(a) rozsah a hranice organizací byly stanoveny a sděleny společné odpovědné osobě;

(b) požadavky tohoto nařízení byly sděleny společné odpovědné osobě a sdíleny s ní;

(c) společná odpovědná osoba má přímý přístup k odpovědnému vedoucímu nebo v případě projekčních organizací – k vedoucímu projekční organizace;

(d) problémy jsou proaktivně řízeny a jakékoli rané varovné signály neshody jsou dokumentovány a jedná se podle toho.

GM1 IS.D.OR.240(e) Požadavky na personál

SPOLEČNÁ ODPOVĚDNÁ OSOBA

Je-li odpovědným vedoucím nebo v případě projekčních organizací – vedoucím projekční organizace pro činnosti podle tohoto nařízení pověřena společná odpovědná osoba (CRP), mělo by být této osobě rovněž přiděleno příslušné pověření, které je nezbytné k tomu, aby implementovala ustanovení IS.D.OR.200, včetně pravomocí a finančních prostředků k mobilizaci a řízení zdrojů napříč organizacemi nebo částmi dotčené organizace. Toto pověření může rovněž zahrnovat jmenování osoby nebo skupiny osob uvedených v IS.D.OR.240(b) a (c) a obecně může CRP při plnění jeho/jejích povinností pomáhat další personál.

Možnost pověření CRP se vztahuje na organizaci, která 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, a proto se očekává, že tato CRP bude mít zodpovědnosti a kompetence v oblasti informační bezpečnosti. Zejména by CRP měla být schopna řídit strategii bezpečnosti informací úřadu a její implementaci, aby bylo zajištěno dosažení cílů popsaných v článku 1. Podle Evropského rámce dovedností v oblasti kybernetické bezpečnosti – *European Cybersecurity Skills Framework* (ECSF) zveřejněného agenturou ENISA v září 2022 může být tato osoba popsána například jako: (vedoucí) manžer informační bezpečnosti ((C)ISO), ředitel programu pro kybernetickou bezpečnost nebo manažer pro bezpečnost informací. Je však třeba poznamenat, že tyto popisy a související dovednosti nezohledňují hledisko bezpečnosti letectví požadované v článku 1.

Pokud je subjekt držitelem více oprávnění nebo prohlášení, mohou příslušní odpovědní vedoucí nebo v případě projekčních organizací – příslušný vedoucí projekční organizace pověřit stejnou CRP, která tedy bude zodpovědná za implementaci ustanovení IS.D.OR.200 pro funkční cluster sdílející struktury, politiky, procesy a procedury v oblasti bezpečnosti informací.

AMC1 IS.D.OR.240(f) Požadavky na personál

DOSTATEČNÝ POČET PRACOVNÍKŮ

Pro určení dostatečnosti personálu je třeba vzít v úvahu následující prvky:

(a) organizační struktury, zásady, procesy a postupy podléhající řízení bezpečnosti informací;

(b) rozsah požadované koordinace s ostatními organizacemi, kontraktory a dodavateli;

(c) míru rizika spojeného s organizací vykonávanými činnostmi.

GM1 IS.D.OR.240(f) Požadavky na personál

DOSTATEČNÝ POČET PRACOVNÍKŮ

Pro účely tohoto nařízení se personálem rozumí kombinace pracovníků přímo zaměstnaných organizací a smluvního personálu, jak je uvedeno v IS.D.OR.235.

Činnosti uvedené v Dodatku II, týkající se hlavních úkolů vyplývajících z provádění Části IS, by měly být zohledněny při vytváření organizační struktury nezbytné pro splnění požadavků tohoto nařízení.

AMC1 IS.D.OR.240(g) Požadavky na personál

NEZBYTNÁ ZPŮSOBILOST (KOMPETENCE)

(a) Pro určení způsobilosti (kompetence) potřebné u personálu provádějící tyto činnosti by měly být vzaty v úvahu následující prvky:

(1) pracovní role a související úkoly;

(2) požadované znalosti, dovednosti a schopnosti.

(b) V rámci procesu, který má zajistit, aby si pracovníci zachovali nezbytnou způsobilost (kompetenci), by měla organizace:

(1) posoudit kvalifikaci a praxi personálu s ohledem na požadovanou způsobilost (kompetenci) pro přidělené pracovní role s cílem identifikovat mezery (slabá místa);

(2) sladit kvalifikaci a praxi personálu s očekávanou způsobilostí (kompetencí) plnit své role organizováním odpovídajících vzdělávacích programů pro stávající členy personálu, náborem nových zdrojů nebo jejich kombinací;

(3) udržovat způsobilost (kompetence) personálu po dobu, po kterou jsou zařazeni do pracovní role.

GM1 IS.D.OR.240(g) Požadavky na personál

NEZBYTNÁ ZPŮSOBILOST (KOMPETENCE) A PROGRAM VÝCVIKU

Program výcviku by měl začínat identifikací způsobilosti (kompetence) vyžadované u personálu pro každou roli, následovanou identifikací mezer (slabých míst) mezi způsobilostí (kompetencí) stávající a požadovanou.

Za účelem vytvoření seznamu způsobilostí (kompetencí) může organizace použít jako počáteční vodítko stávající rámec kompetencí v oblasti kybernetické bezpečnosti, jako je NICE *(National Initiative for Cybersecurity Education)* založený na rámci kybernetické bezpečnosti NIST – *NIST Cybersecurity Framework* (NIST CSF).

V Dodatku II jsou uvedeny hlavní úkoly tohoto nařízení a namapovány na způsobilosti (kompetence) odvozené od NIST CSF. Toto mapování lze použít k vytvoření základní linie pro identifikaci výše uvedených mezer (slabých míst) ve způsobilostech (kompetencích). Je však třeba poznamenat, že stávající rámce způsobilosti (kompetencí) v oblasti kybernetické/informační bezpečnosti, jako je NICE, se obvykle zaměřují především na ochranu standardních informačních technologií; navrhovaný seznam způsobilostí (kompetencí) proto může být nutné přizpůsobit technologiím nebo integrovat do procesů, které jsou používány v organizaci.

Překlenutí zjištěných mezer (slabých míst) by mělo být chápáno jako cíl programu výcviku, který by měl dále zahrnovat rozsah, obsah, metody poskytování (např. školení v učebně (classroom), e-learning, notifikace, zácvik na pracovišti (OJT)) a četnosti školení, které nejlépe odpovídají potřebám organizace s ohledem na velikost, rozsah, požadované kompetence a složitost organizace.

A konečně, jak se informační/kybernetická bezpečnost vyvíjí v důsledku nárůstu nových hrozeb, měla by organizace adekvátnost programu výcviku pravidelně přezkoumávat.

AMC1 IS.D.OR.240(h) Požadavky na personál

UZNÁNÍ POVINNOSTÍ

Pokud jde o jakoukoli přidělenou roli a úkol, organizace by měla jasně a transparentně specifikovat všechny odpovědnosti za bezpečnost informací, které má zaměstnanec.

V rámci toho by všichni pracovníci vykonávající činnosti požadované tímto nařízením měli dohledatelným a ověřitelným způsobem potvrdit, že rozumí přiděleným rolím a souvisejícím povinnostem (odpovědnostem) v oblasti bezpečnosti informací.

GM1 IS.D.OR.240(h) Požadavky na personál

UZNÁNÍ POVINNOSTÍ

Potvrzení o přijetí, jako je platný elektronický podpis nebo vlastnoruční podpis na papíře, potvrzovací e-mail atd., je dohledatelným důkazem potvrzení.

AMC1 IS.D.OR.240(i) Požadavky na personál

TOTOŽNOST A DŮVĚRYHODNOST

U personálu, který má přístup k informačním systémům a datům podléhajícím požadavkům Části IS, by měla být identita určena na základě listinných důkazů.

K prokázání důvěryhodnosti tohoto personálu by organizace měla mít zdokumentovaný proces a vhodná kritéria, která zajistí, že jednotlivcům je možné při výkonu jejich role důvěřovat.

GM1 IS.D.OR.240(i) Požadavky na personál

TOTOŽNOST A DŮVĚRYHODNOST

(a) Důvěryhodnost lze prokázat například:

(1) před nástupem do zaměstnání – ověřením spolehlivosti provedeném v souladu s platnými předpisy unijního a vnitrostátního práva. Toto ověření může zahrnovat verifikaci:

(i) vzdělání, předchozích zaměstnání a případných mezer v předchozích letech;

(ii) absence záznamu v rejstříku trestů;

(iii) jakékoli další relevantní informace nebo zpravodajské informace považované za relevantní pro vhodnost osoby pro práci v předpokládané roli;

(2) v průběhu zaměstnání – sledování věrnosti závazkům a chování zaměstnance.

Poznámka: Absenci záznamu v rejstříku trestů lze ověřit prostřednictvím osvědčení vydaného odpovědným orgánem v členském státě v souladu s nařízením (EU) 2016/1191. V případě potenciálních zahraničních zaměstnanců mohou být výše uvedená ověření prováděna na základě rovnocenných osvědčení vydaných zemí původu, jako je „výpis z rejstříku trestů *(certificate of good conduct)*“.

(b) V případě procesu a kritérií pro stanovení důvěryhodnosti personálu bude možná potřeba dále zvážit, zda:

(1) informační systémy a data, ke kterým se má přistupovat, se při procesu posouzení rizik podle IS.D.OR.205 pojily s vysokou závažností bezpečnostních důsledků;

(2) kontroly nebo zmírňující opatření k řešení rizik identifikovaných během analýzy rizik závisí na organizačních/provozních postupech – například na správné konfiguraci a správě informačních technologií, databázových operacích, monitorování bezpečnosti informací atd.

V takových případech může personál, který má práva administrátora nebo nekontrolovaný a neomezený přístup k systémům a datům uvedeným výše v bodě (a)(1), nebo personál, který uplatňuje opatření podle výše uvedeného bodu (b)(2), podléhat přísnějším kritériím.

(c) Zpravodajské a jakékoli další relevantní informace lze shromažďovat prověřováním a analýzou veřejných zdrojů, jako jsou sociální média a webové stránky, v rámci mezí stanovených příslušnými vnitrostátními zákony a předpisy.

(d) Na některé organozace podle Části IS se také může vztahovat nařízení (EU) 2015/1998, které vyžaduje u personálu v určitých rolích úspěšné absolvování ověření spolehlivosti, jakož i mechanismus pro průběžný přezkum těchto ověření. V takových případech může organizace

k prokázání totožnosti a důvěryhodnosti personálu požadovaných v Části IS, ve vztahu k jejich roli, za vhodné považovat proces a příslušná kritériím definované v nařízení (EU) 2015/1998 pro standardní a důkladnější ověření spolehlivosti. Je však třeba poznamenat, že vyhovění požadavkům na prokázání totožnosti a důvěryhodnosti podle Části IS nepředstavuje vyhovění požadavkům na ověření spolehlivosti, jak jsou definovány v nařízení (EU) 2015/1998.

GM1 IS.D.OR.245 Vedení záznamů

Záznamy jsou vyžadovány k dokumentaci dosažených výsledků nebo k doložení provedených činností. Záznamy se po zaznamenání stávají faktickými a nelze je upravovat. Proto nepodléhají kontrole verzí. I když je vytvořen nový záznam týkající se stejného problému, předchozí záznam zůstává platný.

„Obdržená oprávnění“ uvedená v bodě (a)(1)(i) zahrnují jakékoli „osvědčení“, které organizace obdržela, pokud je to stanoveno prováděcím pravidlem pro její doménu.

AMC1 IS.D.OR.245(a)(1)(vi)&(a)(5) Vedení záznamů

Při plnění požadavků podle bodů (a)(1)(vi) a (a)(5) by organizace měla zavést politiku uchovávání dat definující postupy pro:

(a) správu příslušných souborů dat bezpečnosti informací;

(b) stanovení pravidelného posouzení jejich obsahu; a

(c) definování kritérií umožňujících vymazání záznamů o událostech bezpečnosti informací, pokud byl splněn cíl požadavku (a)(5).

GM1 IS.D.OR.245(a)(1)(vi)&(a)(5) Vedení záznamů

Cílem požadavku (a)(1)(vi) je zajistit detekci možného náznaku incidentů nebo zranitelností v oblasti bezpečnosti informací, které nejsou zřejmé při běžném provozu (např. dříve neznámé situace), zatímco cílem požadavku podle (a)(5) je umožnit nezbytnou flexibilitu při řízení objemu uložených událostí bezpečnosti informací.

Záznamy o událostech bezpečnosti informací zahrnují ty události, které byly identifikovány v rámci detekčních činností podle IS.D.OR.220(a), jakož i další data bezpečnosti informací vytvořená aktivy, která byla identifikována podle IS.D.OR.205.

Politika uchovávání dat objasňuje, jaké informace by měly být uchovávány nebo archivovány a jak dlouho. Některé pokyny k uchovávání dat lze nalézt v dokumentu EUROCAE ED-206, Chapter 2.6.

Jakmile dataset dokončí dobu uchovávání, lze jej smazat nebo přesunout jako trvalá historická data do sekundárního nebo terciárního úložiště.

AMC1 IS.D.OR.245(c)&(d) Vedení záznamů

Při plnění požadavků podle bodů (c) a (d) pro všechny záznamy požadované v bodech IS.D.OR.245 (a) a (b) by organizace měla zvážit následující:

(a) Záznamy by měly být uchovávány v papírové podobě nebo v elektronické podobě nebo v kombinaci obou médií. Záznamy by měly zůstat přístupné, kdykoli je to potřeba, v přiměřené době a použitelné po celou požadovanou dobu uchovávání. Doba uchovávání začíná okamžikem vytvoření záznamu.

(b) Integrita, dostupnost a autenticita dat záznamů by měla být chráněna v souladu s ochranou odpovídajících provozních dat a jako taková by měla spadat do působnosti ISMS.

(c) Úložné systémy by měly být chráněny před neoprávněným přístupem (tj. pokusy o únik dat osobních údajů/úpravy záznamů), a proto by měly mít implementována opatření pro bezpečnost informací v souladu s úrovní rizika bezpečnosti informací, které je s nimi spojeno.

(d) Jakmile již záznamy nemusí být uchovávány, mělo by být náležitě provedeno zničení záznamů a vyřazení majetku používaného k jejich uložení.

GM1 IS.D.OR.245(c)&(d) Vedení záznamů

PŘÍSTUPNOST ZÁZNAMŮ PO CELOU DOBU UCHOVÁVÁNÍ

Doporučuje se dodržovat osvědčené postupy pro uchovávání dat, v případě dat, která může být nutné obnovit, strategie zálohování, jako je použití automatických nástrojů zálohování, segregaci nebo geografickou separaci míst úložišť záloh, a zvážit offline zálohování s cílem zabránit rizikům ransomwaru. Tyto postupy by měly být zváženy také tehdy, když je vedení záznamů smluvně zajištěno poskytovateli služeb s distribuovanými zdroji.

Zvláštní pozornost by měla být věnována významným změnám hardwaru a softwaru, aby se zajistilo, že uložené digitální záznamy zůstanou přístupné a čitelné (např. systém souborů, formát souborů aplikace, dopředně kompatibilní verze databáze atd.). Papírové informace je třeba archivovat v adekvátním prostředí, ve kterém jsou záznamy chráněny před degradačními faktory (např. nadměrným teplem, světlem nebo vlhkostí).

INTEGRITA DAT ZÁZNAMŮ A OCHRANA PROTI NEOPRÁVNĚNÉMU PŘÍSTUPU

Běžně používanou metodou k dosažení ochrany autenticity a integrity je použití digitálních podpisů na úrovni dokumentu. Do souboru dokumentu (např. PDF) lze přidat digitální podpisy, aby bylo zajištěno, že záznam nebyl upraven někým jiným než jeho autorem (integrita) a že autor je, kdo se očekává, že má být (autenticita).

Kromě toho, aby se zabránilo neoprávněnému přístupu, lze záznamy chránit například implementací metody řízení přístupu na základě role – *role-based access control* (RBAC) nebo lze určité záznamy chránit heslem na úrovni souborů. Komerční aplikace obsahují vestavěné základní funkce ochrany heslem pro jejich formáty souborů. Ochrany přístupu lze také dosáhnout ochranou prostředí, kde jsou jednotlivé záznamy uloženy (např. ochrana přístupu k databázím, sdíleným souborům, adresářům atd.).

GM1 IS.D.OR.250(a) Příručka pro řízení bezpečnosti informací (ISMM)

Organizace se může rozhodnout dokumentovat některé informace požadované podle bodu IS.D.OR.250(a) v samostatných dokumentech (např. postupy). V tomto případě by měla zajistit, aby příručka obsahovala odpovídající odkazy na jakýkoli dokument uchovávaný samostatně. Všechny takové dokumenty je pak třeba považovat za nedílnou součást příručky systému řízení bezpečnosti informací organizace.

V případě, že je subjekt držitelem více oprávnění nebo prohlášení, může ISMM platit pro jednu nebo více organizací současně na základě společného ISMS. Tato ISMM by měla obsahovat alespoň schvalovací dokument každé organizace a měla by být formálně schválena odpovědným vedoucím každé organizace nebo v případě projekčních organizací – každým vedoucím projekčních organizací nebo odpovědnou osobou. Společná odpovědná osoba může být jmenována podle IS.D.OR.240(d) a pokynů GM1 IS.D.OR.240(e).

Aby bylo zajištěno, že všechny zúčastněné strany mohou plnit své povinnosti, doporučuje se, aby všechny příručky, postupy a komunikace mezi nimi byly přinejmenším v jednom společném jazyce, např. angličtině. Mezi tyto zúčastněné strany patří příslušné úřady, s nimiž by měl být společný jazyk dohodnut.

AMC1 IS.D.OR.255 Změny systému řízení bezpečnosti informací

Aniž je dotčeno oznamování změn, jak je požadováno pro každou organizaci v odpovídajícím prováděcím nařízení pro oblast uvedenou v čl. 2 odst. 1 nařízení (EU) 2022/1645, postup uvedený v IS.D.OR.255(a)(1) by měl při navrhování způsobu, jakým budou řízeny, zohledňovat kritičnost daných změn. Zejména ty změny, které by mohly mít dopad na dosažení nebo udržení souladu s ustanoveními Části IS nebo které by mohly vést k nepřijatelné úrovni rizika (např. podle pokynů uvedených v GM1 IS.D.OR.205(c)), by měly být podrobeny kontrole. Po zavedení tohoto postupu by jakékoli jeho další změny měly podléhat schválení příslušným úřadem.

Pokud je požadováno předchozí schválení od příslušného úřadu pro změnu, na kterou se nevztahuje schválený postup, nebo pokud takový schválený postup neexistuje, měla by organizace poskytnout alespoň tyto informace:

— povaha a účel změny;

— plán implementace změny;

— plán ověření změny;

— potenciální dopad na bezpečnost letectví, který změna přináší.

Významná odchylka od původního plánu implementace během procesu změny je událost, která by měla být hlášena příslušnému úřadu, protože tato odchylka může vyžadovat přehodnocení dopadu změny.

GM1 IS.D.OR.255 Změny systému řízení bezpečnosti informací

Bod IS.D.OR.255 má následující strukturu:

Bod (a) zavádí možnost, aby se organizace dohodla s příslušným úřadem, že změny ISMS mohou být implementovány bez předchozího schválení, pokud se na tyto změny vztahuje postup pro změny.

Bod (b) zavádí povinnost předchozího schválení (příslušným úřadem) v případě změn, na které se nevztahuje výše uvedený postup, a uvádí, jak by mělo být s těmito změnami naloženo.

Organizace by měla zvážit zavedení postupu pro řízení a oznamování změn příslušnému úřadu, jak je stanoveno v IS.D.OR.255(a). V případě neexistence jakéhokoli schváleného postupu bude muset organizace pro jakoukoli změnu požádat o schválení a získat jej, jak je požadováno v IS.D.OR.255(b). V každém případě by všechny změny měly být při implementaci oznámeny příslušnému úřadu.

GM2 IS.D.OR.255 Změny systému řízení bezpečnosti informací

VZTAH MEZI ZMĚNAMI ISMS A SOUSTAVNÝM ZLEPŠOVÁNÍM

Změny vyplývající z procesu neustálého zlepšování stanoveného organizací (viz IS.D.OR.260) by měly být řešeny jako jakákoli jiná změna podle pokynů v AMC1 IS.D.OR.255 a GM1 IS.D.OR.255.

PŘÍKLAD ZMĚN, KTERÉ MOHOU MÍT DOPAD NA ISMS

Níže jsou uvedeny některé příklady změn, které mohou mít dopad na ISMS nebo které by mohly vést k nepřijatelné úrovni rizika, a proto by měly podléhat kontrole ze strany příslušného úřadu podle ustanovení stanovených v IS.D.OR.255:

(a) Změny rozsahu ISMS, rozhraní nebo souvisejících politik:

— Organizace rozšiřuje působnosti svého podnikání a integruje další společnost do své organizační struktury.

— Organizace identifikovala neshody naznačující nesprávný rozsah.

— Organizace mění svou politiku a/nebo cíle v oblasti bezpečnosti informací s potenciálním dopadem na bezpečnost letectví.

— Změny rozhraní organizace vyplývající např. ze změn v insourcovaných nebo outsourcovaných činnostech.

(b) Změny v zodpovědnostech a odpovědnosti, jakož i v organizační struktuře zahrnující implementaci a průběžné sledování souladu s tímto nařízením:

— Odpovědný vedoucí delegoval určité povinnosti podle Části IS na osobu nebo skupinu osob.

— Organizace uzavírá smlouvy na činnosti týkající se řízení bezpečnosti informací podle IS.D.OR.235.

(c) Změny používané metodiky řízení rizik:

— Organizace mění klasifikaci pravděpodobnosti nebo dopadů ve své metodice řízení rizik, např. s cílem získat vyšší rozčlenění.

— Organizace implementuje změny ve své metodice řešení rizik.

— Organizace integruje své řízení rizik v oblasti bezpečnosti informací do stávajících systémů řízení.

(d) Změny v procesu správy událostí v oblasti bezpečnosti (security):

— Organizace se rozhodne smluvně zajišťovat činnosti týkající se správy událostí v oblasti bezpečnosti (security).

— Organizace mění proces oznamování událostí v oblasti bezpečnosti (security) a kritéria tak, aby eskalovala k vyššímu vedení pro rychlejší řešení.

— Organizace mění svou politiku pro zmírňování zranitelností.

— Organizace mění svůj postup pro zotavení se (obnovu) z incidentu.

PŘÍKLAD ZMĚN, KTERÉ NEMAJÍ DOPAD NA ISMS

Ne všechny provozní změny související s bezpečností informací mají dopad na ISMS, a proto se ne všechny změny musí hlásit příslušnému úřadu v souladu s ustanoveními uvedenými v IS.D.OR.255. Takovéto změny mohou reprezentovat následující scénáře:

— Po úspěšně detekované události v oblasti bezpečnosti (security), která se mohla snadno vyvinout v incident, se organizace rozhodne spustit rozsáhlou kampaň na zvýšení povědomí o kybernetické bezpečnosti pro všechny zaměstnance.

— Aktualizace programu školení personálu a/nebo obsahu školení jako výsledek procesů neustálého zlepšování zavedených v organizaci.

— Organizace nahrazuje softwarový nástroj, který používá pro šifrování citlivých souborů, jiným softwarovým řešením.

— Organizace se rozhodla provést vnitřní restrukturalizaci z obchodních důvodů, změnit názvy oddělení nebo sekcí, aniž by provedla jakékoli změny v zodpovědnostech a odpovědnosti (např. odpovědný vedoucí) zahrnující ISMS organizace.

— Organizace se rozhodne aktualizovat stávající preventivní kontrolu, např. konfiguraci nového firewallu ve své vnitřní síti.

AMC1 IS.D.OR.260 Soustavné zlepšování

Proces neustálého zlepšování (CIP), jak vyžaduje IS.D.OR.200(b), by se měl zaměřit na soustavné zlepšování účelnosti, vhodnosti a přiměřenosti ISMS. Toho by mělo být dosaženo proaktivním a systematickým posuzováním ISMS a všech jeho prvků – včetně jeho vyspělosti. Posuzování by mělo zohlednit výsledky a závěry dalších procesů bezpečnosti a zajištění informací, včetně auditů, přezkoumání vedením, hodnocení výkonnosti, účelnosti a vyspělosti, jakož i výsledky odvozených nápravných opatření a náprav.

Kroky, které je třeba provést, by měly být alespoň následující:

(a) Identifikace příležitostí ke zlepšení na základě výsledků posouzení ISMS s ohledem na jeho vhodnost, účelnost, přiměřenost, a je-li to považováno za nutné, i efektivnost, jakož i na jakýkoli jiný návrh na zlepšení. Posouzení by mělo vzít v úvahu ukazatele výkonnosti, které odrážejí jeho procesy a prvky a definované cíle účelnosti a vyspělosti.

(b) Vyhodnocení identifikovaných příležitostí z hlediska nákladů a přínosů, absence nebo snížení nežádoucích účinků a dosažení plánovaných cílů a zamýšlených výsledků.

(c) Návrh vyhodnocených možností zlepšení vedení a doporučení činností k podpoře jejich přezkoumání a rozhodování.

(d) Podle rozhodnutí přijatého podle bodu (c) výše – plánování, vývoj a implementace činností a změn ISMS, jeho procesů nebo prvků k dosažení zlepšení.

(e) Vyhodnocení účelnosti realizovaných opatření a změn ISMS a případně ověření, že byla odstraněna kořenová příčina zjištěných nedostatků.

Vedení by mělo v plánovaných intervalech posuzovat a přezkoumávat výsledky CIP, aby zajistilo trvalou účelnost, přiměřenost a vhodnost ISMS, rozhodlo o prioritách provádění činností a změn, jakož i revidovalo nebo stanovilo nové cíle, nebo cíle pro neustálé zlepšování.

GM1 IS.D.OR.260 Soustavné zlepšování

Bod IS.D.OR.260 pokrývá procesy zajištění pro ISMS způsobem, který lze považovat za rovnocenný zajištění bezpečnosti v dokumentu ICAO Doc 9859 „*Safety Management Manual (SMM)*“, který zahrnuje sledování a měření výkonnosti, řízení změn a neustálé zlepšování SMS.

V tomto nařízení:

— IS.D.OR.260(a) se za použití přiměřených ukazatelů výkonnosti zabývá posuzováním účelnosti a vyspělosti ISMS;

— IS.D.OR.260(b) řeší opatření ke zlepšení, tj. nápravy a nápravná opatření, pro nedostatky zjištěné v IS.D.OR.260(a) a proces neustálého zlepšování.

Podobná ustanovení pro neustálé zlepšování jsou obsažena v jiných systémech řízení informací, jako je ISO/IEC 27001 (viz Dodatek II k tomuto dokumentu).

Kontext a prostředí rizik organizací nejsou nikdy statické, a proto vyžadují dynamické přizpůsobení, vývoj a změnu cílů, architektur, organizačních struktur a procesů dané organizace, aby byla rizika bezpečnosti informací udržována na přijatelné úrovni. V důsledku toho by měl být ISMS považován za vyvíjející se a učící se část/prvek organizace, který je třeba neustále monitorovat a zlepšovat, s cílem zajistit sladění s bezpečnostními cíli organizace a účelnost.

CIP si klade za cíl neustále zlepšovat účelnost, vhodnost, přiměřenost a v případě potřeby i effektivnost ISMS. Organizace může začlenit CIP podle Části IS do některých jiných již působících CIP a může použít metody, jako je cyklus plánuj-dělej-kontroluj-jednej (PDCA) *(Plan-Do-Check-Act)* nebo cyklus definuj-měř-analyzuj-vylepši-kontroluj (DMAIC) *(Define-Measure-Analyse-Improve-Control)* (viz také GM1 IS.D.OR.200).

CIP je založen na proaktivním a systematickém posuzování ISMS a všech jeho prvků včetně procesů a kontrol bezpečnosti informací řízených ISMS. Posouzení by mělo být provedeno podle organizačních cílů pro požadované úrovně výkonu, účelnosti a vyspělosti. Tyto cíle, kromě zajištění dosažení vyhovění požadavkům podle tohoto nařízení, mohou také zahrnovat cíle stanovené politikou nebo normami dané organizace a rozhodnutími vedení.

Výše uvedené posouzení je založeno na výsledcích hodnocení výkonnosti, auditů, rizikových a incidentních procesů, jakož i již aplikovaných nápravných opatření a náprav. Některé faktory, které je třeba vzít v úvahu při provádění posouzení, jsou následující:

— **Přiměřenost** se týká toho, zda systém zavádí disciplíny potřebné pro řízení bezpečnosti informací, např. používáním široce uznávaných průmyslových norem, dostatečným způsobem s ohledem na vyhovění požadavkům tohoto nařízení.

— **Účelnost ISMS** a efektivní implementace procesů a kontrol řízených ISMS se posuzuje analýzou, zda:

  — rizika v oblasti bezpečnosti informací jsou řízena tak, aby bylo dosaženo bezpečnostních cílů;

  — bylo dosaženo zamýšlených výsledků ISMS a byly splněny požadavky nebo cíle;

  — všechny typy nedostatků, včetně poruch, jsou řízeny tak, aby splnily nebo správně implementovaly požadavek nebo kontrolu.

— **Efektivita** ISMS se týká implementace zjednodušených procesů; zlepšení efektivity by však neměla mít nepříznivý dopad na účelnost.

Identifikace příležitostí ke zlepšení

Příležitosti ke zlepšení mohou být identifikovány z výsledků posuzování CIP nebo mohou být předloženy jako návrhy z jiných zdrojů. Identifikace často zahrnuje odchylky nebo nápravná opatření, stejně jako neefektivní procesy nebo kontroly, které nejsou napraveny.

Návrhy na zlepšení pocházejí ze zdrojů, jako jsou:

— Řízení rizik: primárním faktorem zlepšování ISMS jsou výsledky pravidelných analýz rizik a následných řešení rizik, kdy proces řešení rizik zahrnuje sledování implementovaných bezpečnostních opatření a vyhodnocování jejich účelnosti.

— Hodnocení výkonnosti a účelnosti: závěry z (klíčových) ukazatelů výkonnosti, jejich měření, analýza a průběžné monitorování a také výsledek posouzení účelnosti včetně výsledků následně aplikovaných náprav a nápravných opatření.

— Hodnocení vyspělosti včetně výsledků následných náprav a nápravných opatření.

— Ponaučení získaná z procesu detekce, zpracování a reakce na incidenty v oblasti bezpečnosti informací a potenciální řešení kořenové příčiny.

— Výsledky (interních) auditů lze použít k ověření, zda ISMS a kontroly v rámci rozsahu auditu splňují požadavky dané organizace, a ke zjištění, kde existují potenciální oblasti pro zlepšení.

— Přezkoumání a vyhodnocení ze strany vedení současného akčního plánu, stanovení nebo revize cílů nebo rozhodnutí o příležitostech a opatřeních ke zlepšení.

— Program návrhů organizace (návrhy na zlepšení), přezkoumání, průzkumy nebo hodnocení se zaměstnanci nebo zpětná vazba od dodavatelů nebo styčných stran.

Jakýkoli výsledek tohoto procesu by měl být zdokumentován. Výsledná opatření mohou být začleněna do zastřešujícího akčního plánu, který je centrálně konsolidován a pravidelně přezkoumáván podle příslušných politik. Výsledný akční plán lze dále rozdělit na taktický, krátkodobý/střednědobý akční plán a strategický, dlouhodobý akční plán.

AMC1 IS.D.OR.260(a) Soustavné zlepšování

(a) **POSOUZENÍ ÚČELNOSTI ISMS**

Při plnění požadavků IS.D.OR.260(a) by organizace měla mít zaveden proces monitorování, měření, hodnocení a přezkoumání účelnosti svého ISMS, který definuje:

(1) kdo monitoruje, měří, analyzuje a vyhodnocuje výsledky a přijímá odpovědná rozhodnutí;

(2) kdy by měly být provedeny výše uvedené kroky;

(3) jaké metody monitorování, měření, analýzy a hodnocení se používají k zajištění srovnatelných a reprodukovatelných výsledků.

Kalendářní základ posuzování by měl být úměrný maximální úrovni rizika stanovené v IS.D.OR.205.

Proces monitorování, měření, hodnocení a přezkoumávání účelnosti ISMS organizace uvedený v AMC1 IS.D.OR.260(a) by měl zahrnovat minimálně:

(1) shromažďování a uchovávání metrik činností a dalších informací, které by mohly být užitečné pro účely monitorování;

(2) analýzu metrik za účelem identifikace trendů a odchylek od předem definovaných výkonnostních cílů.

(b) **POSOUZENÍ VYSPĚLOSTI ISMS**

Organizace by měla posoudit vyspělost svého ISMS pomocí vhodného modelu vyspělosti, aby identifikoval oblasti pro zlepšení ISMS. K tomu by měla organizace:

(1) definovat nebo přijmout model vyspělosti, který představuje soubor důležitých a relevantních procesů a schopností, jejichž implementace a udržování se očekává;

(2) pro každý posuzovaný proces nebo schopnost zajistit, aby model definoval kritéria, podle kterých by měly být při určování úrovně vyspělosti posuzovány a hodnoceny specifické aspekty, charakteristiky a účelnost;

(3) definovat pro každý posuzovaný proces nebo schopnost jejich požadovanou cílovou úroveň vyspělosti.

(c) Pro každý posuzovaný proces nebo schopnost v oblasti bezpečnosti informací obsažené v modelu vyspělosti by organizace měla:

(1) vyhodnotit a zdůvodnit aktuální úroveň vyspělosti;

(2) identifikovat jakoukoli oblast pro zlepšení, které by měl učinit, aby dosáhl cílové úrovně vyspělosti;

(3) shromažďovat a zaznamenávat důkazy o silných a slabých stránkách implementovaného ISMS a jeho vyhodnocené vyspělosti.

GM1 IS.D.OR.260(a) Soustavné zlepšování

(a) Jako obecné vodítko by prvky ISMS, které by měly být monitorovány, měřeny a hodnoceny, měly být minimálně:

(1) proces posuzování a řešení rizik (včetně rizik na rozhraních s jinými organizacemi);

(2) řízení neshod a nápravných opatření;

(3) řízení incidentů a zranitelností;

(4) řízení způsobilosti (kompetencí) persoálu.

(b) Existující modely vyspělosti pro hodnocení ISMS

Jako obecné vodítko pro definici nebo přijetí modelu vyspělosti *(maturity model)*(MM) lze zvážit následující existující modely:

— *Cybersecurity Capability Maturity Model* (C2M2), verze 1.1: tento model byl zveřejněn Ministerstvem energetiky USA v roce 2014. Zavádí pojem úrovně indikátoru splatnosti − *Maturity Indicator Levels* (MIL) v rozsahu od 0 do 3 a zabývá se nejen úrovněmi výkonnosti, ale také postupy provedení (v rámci cílů přístupu a progrese přístupu) a také postupy zajištění (v rámci cílů řízení a progrese institucionalizace).

— *Systems Security Engineering – Capability Maturity Model* (SSE-CMM): zveřejněn organizací ISO jako ISO 21827 v roce 2008. Zaměřuje se na inženýrské postupy, mnohem méně na provozní postupy, které jsou rozděleny do 11 „základních bezpečnostních postupů − *Security Base Practices*“ a 11 „základních projektových a organizačních postupů − *Project and Organizational Base Practices*“. Zavádí pojem pěti úrovní schopností, od „neformálně prováděné − *Performed Informally*“ po „neustále se zlepšující − *Continuously Improving*“.

— *NIST Cybersecurity Framework* (NIST CSF), verze 1.1: zveřejněn institutem NIST v dubnu 2018. Ačkoli není navržen jako MM, rámec definuje čtyři „implementační úrovně − *Implementation Tiers*“, od „částečné − *Partial*“ po „adaptivní − *Adaptive*“, které jsou kvalitativním měřítkem organizačních postupů řízení rizik kybernetické bezpečnosti. Zaměřuje se na funkčnost a opakovatelnost řízení rizik kybernetické bezpečnosti.

— *ATM Cybersecurity Maturity Model*, edice 1: publikován v únoru 2019 EUROCONTROL NM pro organizace v oblasti ATM. I když není navržen pro širší použití, lze jej podle potřeby upravit. Definuje pět úrovní vyspělosti, od „neexistující − *Non-existent*“ po „adaptivní − *Adaptive*“, inspirované terminologií „Tier“ z NIST CSF. Ve skutečnosti je model založen na NIST CSF spolu s některými prvky ISO/IEC 27001.

Následující Tabulka 1 mapuje výše uvedené MM na hypotetický pětiúrovňový MM.

Tabulka 1: Matice mapování existujícího MM na hypotetický pětiúrovňový MM

Mapování na pětiúrovňový MM	C2M2	Eurocontrol NM	ISO 21827	NIST CSF 1.1
Initial (počáteční)	MIL 0	Non-Existent	Performed Informally	
Defined (definovaná)	MIL 1 (Initial)	Partial	Planned & Tracked	Partail
Implemented (implementovaná)	MIL 2 (Identified)	Defined	Well defined	Risk-Informed
Managed (řízená)	MIL 3 (Managed)	Assured	Quantitatively Controlled	Repeatable
Improved (zlepšená)		Adaptive	Continuously Improving	Adaptive

Není vyžadována žádná konkrétní úroveň vyspělosti. Pokud však bude dosaženo souladu, organizace určí, které požadavky kterých modelů již byly splněny (povinné), a mohou se rozhodnout dosáhnout úrovně, která je pro danou organizaci výhodná (dobrovolné). V dlouhodobějším horizontu může dosažení vyšších úrovní vyspělosti zvýšit důvěru úřadů dozoru, což může mít dopad na úroveň činností dozoru týkajících se takovéto organizace.

AMC1 IS.D.OR.260(b) Soustavné zlepšování

Pokud je zjištěn nedostatek, měla by organizace včas reagovat podle definovaného procesu vedoucího ke zvládnutému (řízenému) stavu, pokud jde o nedostatek, jeho související důsledky a v případě potřeby prevenci jeho budoucího opakování nebo výskytu jinde.

Na základě vyhodnocení dopadu a rozsahu nedostatku a potenciálních důsledků na ISMS by měl proces zahrnovat jako kritéria pro vyhovění:

(a) rozhodování o nápravách a jejich provedení bez zbytečného odkladu za účelem omezení dopadu nedostatku a řešení jeho důsledků a případně jeho kontroly nebo odstranění;

(b) rozhodování o potřebě a provedení nápravných opatření k odstranění příčiny a faktorů přispívajících k nedostatku na základě analýzy kořenové příčiny a vyhodnocení opatření k nápravě příčiny s cílem být úměrné následkům a dopadu nedostatku;

(c) ověřování provedených činností:

(1) aby byly účinné a vedly k přijatelným zbytkovým rizikům;

(2) aby neměly nezamýšlené vedlejší účinky vedoucí k dalším nedostatkům, novým rizikům nebo ISMS, který není v souladu s platnými požadavky; jakož i

(3) aby se v případě nápravných opatření účinně napravila nebo odstranila kořenová příčina;

(d) hlášení a přezkoumávání zjištěných nedostatků, akčního plánu a výsledků opatření přijatých odpovědným vedoucím organizace nebo v případě projekčních organizací – vedoucím projekční organizace, a v případě potřeby s dalšími zúčastněnými nebo dotčenými rolemi a stranami;

(e) dokumentování jako důkazu zjištěných nedostatků, plánovaných a realizovaných náprav a/nebo nápravných opatření spolu s termíny a odpovědnými osobami, zpětné vazby vedení, výsledků procesního kroku podle bodu (c) výše a v případě potřeby rozhodnutí o změně přijaté pro samotný ISMS.

GM1 IS.D.OR.260(b) Soustavné zlepšování

„Nezbytná opatření ke zlepšení“ uvedená v IS.D.OR.260(b) se týkají náprav nebo nápravných opatření k odstranění nedostatků nebo opatření zaměřených na zlepšení účelnosti a vyspělosti ISMS.

Proces splňující kritéria definovaná v AMC1 IS.D.OR.260 by měl zahrnovat následující aspekty:

(a) identifikování rozsahu, dopadu, kontextu a spouštěčů nedostatku, jeho vyhodnocení podle některých stanovených kritérií, analyzování potenciálních důsledků pro ISMS včetně potenciální existence v jiných oblastech;

(b) rozhodování o nápravách a jejich provádění k okamžitému omezení dopadu a zvládání (řízení) následků nedostatku a případně k jeho kontrole nebo odstranění;

(c) rozhodování o nápravných opatřeních nezbytných k odstranění (kořenové) příčiny (příčin) nedostatku, která jsou úměrná následkům;

(d) opětovné posuzování prvků ISMS, které mohou být ovlivněny realizovanými opatřeními, aby se zajistilo, že nevznikne žádné další riziko;

(e) ověřování provedených činností uvedených v bodě (c) AMC1 IS.D.OR.260(b);

(f) hlášení a přezkoumávání výsledků kroků procesu s vedením (viz bod (d) AMC1 IS.D.OR.260(b));

(g) dokumentování a dokládání výsledku výše uvedených procesních kroků (viz bod (e) AMC1 IS.D.OR.260(b)).

Dodatek I
Příklady scénářů hrozeb s potenciálním škodlivým dopadem na bezpečnost

Níže je uveden nevyčerpávající seznam příkladů scénářů hrozeb v oblasti bezpečnosti informací s potenciálním škodlivým dopadem na bezpečnost, které mohou úřady a organizace zvážit.

Příklad 1: Digitální spojení letadlo – ATC

— **Aktiva/doména vektoru hrozby**

  — hlasové a pozemní automatizované systémy ATC

  — poskytovatelé pozemních komunikací

  — poskytovatelé služeb VF spojení letadlo – země / země – letadlo

  — letadla a prostředky používané pro hlasové spojení a komunikaci datovým spojem

— **Nevyčerpávající souhrn potenciálních hrozeb**

  — hrozba (dostupnost): překročení výkonnosti systému, saturace komunikačního kanálu

  — hrozba (integrita): MITM útoky *(man-in-the-middle attack)* nebo útoky typu injekce *(injection attack)*

  — hrozba (důvěrnost): pasivní naslouchání komunikaci, špehování hardwarových zařízení

— **Souhrn scénářů hrozeb a jejich potenciálních škodlivých dopadů na bezpečnost**

  — Narušení služeb brání spojení ATC s jedním nebo více letadly a/nebo pozemním systémem ATC.

  — Manipulace s daty prostřednictvím MITM útoku by pilotovi a/nebo systému ATC poskytla nepravdivé informace, což může vytvořit bezpečnostní riziko, nebo vložení dat do letadla nebo pozemních systémů s cílem narušit službu a schopnosti.

  — Neexistují žádné specifické regulační požadavky na šifrování dat nebo hlasu pro komunikaci datovým spojem; z důvodu zachování důvěrnosti by však zařízení používaná k poskytování a dodávkám služeb měla být kontrolována a omezena pouze na ty zdroje, které vyžadují přístup, aby bylo zajištěno, že služby nemohou být jakýmkoli způsobem narušeny a manipulovány.

Příklad 2: Nedovolená manipulace s daty letového provozu

— **Aktiva/doména vektoru hrozby**

  — poskytovatel internetových služeb (ISP)

  — síť (sítě) služeb ATM

  — přehledová data

  — systémy ATC

— **Nevyčerpávající souhrn potenciálních hrozeb**

  — Kompromitace ISP (confidentiality): Útočník získá neoprávněný přístup k systémům nebo infrastruktuře ISP poskytujícího služby sítě systému ATM.

  — Manipulace s daty (integrita): Jakmile je ISP kompromitován, útočník by mohl manipulovat s daty při přenosu. To by mohlo zahrnovat vložení (injekce) falešných dat nebo odstranění/úpravu dat legitimních.

  — Odmítnutí služby (dostupnost): Útočník by také mohl potenciálně zcela narušit datovou komunikaci, což by mělo za následek odmítnutí služby (DoS) systému.

— Injekce malwaru (integrita/dostupnost): Útočník by mohl potenciálně využít kompromitovaného ISP jako odrazový můstek k vložení malwaru do systémů, což by způsobilo další narušení nebo umožnilo další útoky.

— **Souhrn scénářů hrozeb a jejich potenciálních škodlivých dopadů na bezpečnost**

— Kompromitace ISP: Zachycení citlivých dat a/nebo manipulace s nimi mající dopad na bezpečné řízení letového provozu.

— Manipulace s daty: Nesprávné situační povědomí, které může mít za následek snížení rozstupů mezi letadly a nesprávná rozhodnutí řízení letového provozu.

— Odmítnutí služby: Snížení schopnosti ATC zajišťovat rozstup vedoucí k aktivaci postupů pro nenadálé události, včetně snížení kapacity, s případnou možností uzavření velkých oblastí vzdušného prostoru.

Příklad 3: Dodavatelský řetězec softwaru a pozemní infrastruktura provozovatele letadla, CAMO a organizací k údržbě letadel, včetně vybavení používaného k podpoře řízení, provozu a údržby letadel

— **Aktiva/doména vektoru hrozby**

— dodavatelský řetězec provozovatelů letadel, CAMO a organizací k údržbě

— interní pozemní infrastruktura provozovatele letadla nebo údržby používaná ke správě letadel a provozu (hardware/software) a další aktiva informačních technologií

— aktiva informačních technologií používaná k aktualizaci systémů v letadle (software a hardware) používaných pro činnosti údržby

— **Nevyčerpávající souhrn potenciálních hrozeb**

— hrozba (dostupnost): narušení hardwaru/softwaru/systému

— hrozba (integrita): kompromitovaný hardware/software/systém

— hrozba (důvěrnost): kompromitovaný hardware/software/systém

— **Souhrn scénářů hrozeb a jejich potenciálních škodlivých dopadů na bezpečnost**

— Narušení šíření meteorologických informací, když je letadlo ve vzduchu, může snížit schopnost letové posádky vyhnout se potenciálně nebezpečným meteorologickým podmínkám (např. silným bouřím/mlze v noci).

— Manipulace s navigačními daty/navigační databází bude mít za následek, že letovým plánům a zobrazením navigačních informací nelze věřit.

— Nedostatek kontroly a přístupu k informacím, jako je program údržby flotily nebo plánování letových posádek, ovlivňuje schopnost organizací udržovat bezpečný provoz.

Použití motýlkové analýzy na tento příklad

Kombinují se dvě koordinované motýlkové analýzy různých dimenzí rizik, protože konečný zájem spočívá pouze v důsledcích pro bezpečnost letectví.

Prvek motýlkové analýzy informační bezpečnosti (security)	Prvek motýlkové analýzy bezpečnosti (safety) letectví
Hrozby informační bezpečnosti 1) zneužití zranitelnosti hardwaru/softwaru: narušená funkce systému 2) zneužití zranitelnosti hardwaru/softwaru: kompromitována integrita systému	

Prvek motýlkové analýzy informační bezpečnosti (security)	Prvek motýlkové analýzy bezpečnosti (safety) letectví
3) zneužití zranitelnosti hardwaru/softwaru: kompromitována důvěrnost informací zpracovávaných systémem (systémy)	
Preventivní bariéry informační bezpečnosti	
Nebezpečí & hlavní události informační bezpečnosti 1) narušená funkčnost systému (nebezpečí) → narušená/nespolehlivá funkčnost systému 2) kompromitovaná integrita systému (nebezpečí) → funkce systému nepředvídatelná 3) informace odhalitelné (nebezpečí) → nezjistitelná exfiltrace informací	Hrozby pro bezpečnost 1) narušená/nespolehlivá funkčnost systému 2) funkce systému nepředvídatelná 3) nezjistitelná exfiltrace informací
Zmírňující bariéry informační bezpečnosti	Preventivní bariéry pro bezpečnost 1) použití kontroly přístupu u správy systému 2) atd.
Následky pro informační bezpečnost 1) ztráta funkce systému (= výpadek výrobního systému) 2) ztráta integrity funkce systému (= některá funkce systému chybná/nefunkční) 3) ztráta důvěrnosti informací (= některé informace mohou uniknout)	Nebezpečí & hlavní události pro bezpečnost: 1) ztráta funkce systému (nebezpečí) → *v provozním systému údržby* 2) ztráta integrity funkce systému (nebezpečí) → *systémy pracují s nesprávnými informacemi* 3) ztráta důvěrnosti informací (nebezpečí) → *únik důvěrných informací o údržbě a vnitřku letadla*
	Zmírňující bariéry pro bezpečnost 1) použití záložních postupů, aby se zabránilo chybným úkonům údržby 2) použití postupů k zabezpečení integrity softwaru letadla
	Následky pro bezpečnost 1) chybné úkony údržby 2) nesprávně provedené úkony údržby 3) exfiltrace informací umožňuje identifikaci zranitelností 4) narušení systémů letadla, nepředvídatelná funkce systému, ztráta významných systémů letadla (jako je ovládání motoru)

Příklad 4: Software projekčních a výrobních organizací, dodavatelský řetězec, konstrukční a výrobní pozemní infrastruktura

— **Aktiva/doména vektoru hrozby**

  — dodavatelský řetězec částí, hardwaru a softwaru projekčních a výrobních organizací

  — interní pozemní infrastruktura projekčních a výrobních organizací používaná ke správě softwaru/hardwaru používaných při výrobě a vývoji produktů, které budou používat výrobci letadel, provozovaté nebo prostředky informačních technologií pozemních automatizačních systémů ATM/ANS (hardware/software).

— aktiva informačních technologií projekčních a výrobních organizací používaná jejich zákazníky k aktualizaci systémů v letadle (softwaru/hardwaru) používaných pro úkony údržby nebo pozemních automatizačních systémů ATM/ANS.

— **Nevyčerpávající souhrn potenciálních hrozeb**

— hrozba (dostupnost): systémy používané k ukládání, přenosu a výměně informací jsou kvůli útokům DoS pro zásadní úkony nedostupné

— hrozba (integrita): systémy používané k ukládání, přenosu a výměně informací jsou prostřednictvím MITM útoků kompromitovány

— hrozba (důvěrnost): k systémům používaným k ukládání, přenosu a výměně informací mají přístup vnitřní nebo vnější hrozby

— **Souhrn scénářů hrozeb a jejich potenciálních škodlivých dopadů na bezpečnost**

— Narušení systémů používaných k ukládání, přenosu a výměně informací způsobem, který by bránil řádnému řízení letadla a jeho systémů a nepříznivě ovlivnil provoz letadla.

— Systémy používané k ukládání, přenosu a výměně informací již nelze považovat za důvěryhodné. Pokud nejsou udržovány na takové úrovni, aby bylo zajištěno, že veškerou výměnu informací, data a software lze považovat za důvěryhodné, dojde k přerušení pozemního provozu i provozu letadel.

— Díky nekontrolovanému přístupu k systémům používaným k ukládání, přenosu a výměně informací (včetně informací, které jsou přijímány a vyměňovány s dodavatelským řetězcem) mohou být opatřeny technické detaily, které by mohly být použity k vytvoření sofistikovanějších útoků zaměřených na systémy kritické z hlediska bezpečnosti.

Příklad 5: Systém výcviku

— **Aktiva/doména vektoru hrozby**

— dodavatelský řetězec veškerého softwaru a hardwaru, který bude použit v systémech výcviku nebo výcvikových zařízeních (včetně letových simulátorů) používaných k výcviku pilotů nebo personálu pozemních systémů ATM/ANS

— interní infrastruktura použitá ve veškerém softwaru a hardwaru, který bude použit při návrhu, výrobě nebo produkci produktů (hardwaru nebo softwaru), které budou použity v letadlech nebo pozemních systémech ATM/ANS

— správa interních operačních domén a systému veškerého softwaru a hardwaru, který bude použit při návrhu, výrobě nebo produkci produktů (hardwaru nebo softwaru), které budou použity v letadlech nebo pozemních systémech ATM/ANS

— **Nevyčerpávající souhrn potenciálních hrozeb**

— hrozba (dostupnost): systémy výcviku nebo výcviková zařízení jsou pomocí útoků DoS znepřístupněny, když je potřeba je použít

— hrozba (integrita): systémy výcviku nebo výcviková zařízení jsou prostřednictvím MITM útoků kompromitovány

— hrozba (důvěrnost): k funkčním modelům, informacím a datům, které jsou zabudovány do systémů výcviku nebo výcvikových zařízení, mají přístup vnitřní nebo vnější hrozby

— **Souhrn scénářů hrozeb a jejich potenciálních škodlivých dopadů na bezpečnost**

— Narušení systémů výcviku (hardwaru a softwaru) bude mít dopad na schopnost organizací udržet si kvalifikovaný personál. Rovněž by to zabránilo letadlu a jeho systémům ve správném provozu a ovlivnilo by úkony údržby pozemních systémů ATM/ANS.

— Model výcviku nebo způsoby poruch a související nouzové podmínky se liší od skutečného chování leteckého systému, a proto vyvolávají nepřiměřené reakce. Pokud systémům výcviku nelze důvěřovat, ovlivní to schopnost organizací udržovat dostatečně kvalifikovaný personál pro svůj provoz (piloti, personál údržby nebo pozemní personál ATM/ANS, který prošel nesprávným výcvikem, by měl být rekvalifikován).

— Nedostatek kontroly a přístupu k systémům výcviku ovlivňuje schopnost organizací udržovat systém výcviku, o kterém je známo, že je v důvěryhodném stavu. Navíc nekontrolovaný přístup k systémům výcviku, které obsahují funkční modely, informace a data, může poskytnout technické detaily, které by mohly být použity k vytvoření sofistikovanějších útoků na samotný systém výcviku nebo na systém kritický z hlediska bezpečnosti v reálném světě.

Příklad 6: Letištní systém dodávky paliva a související infrastruktura

— **Aktiva/doména vektoru hrozby**

— pozemní infrastruktura skladování a distribuce paliva

— digitální systémy používané k řízení čerpání a měření množství paliva

— dodavatelský řetězec pro dodávky paliva, včetně dodavatelů paliva třetích stran

— aktiva letištní informační technologie používaná pro řízení zásob paliva a plánování dodávek

— **Nevyčerpávající souhrn potenciálních hrozeb**

— hrozba (dostupnost): přerušení plnění palivem nebo systémů dodávek paliva

— hrozba (integrita): manipulace s palivovými řídicími systémy nebo měřicími zařízeními

— hrozba (důvěrnost): neoprávněný přístup k údajům o plnění palivem a dodávkách paliva

— **Souhrn scénářů hrozeb a jejich potenciálních škodlivých dopadů na bezpečnost**

— Přerušení dodávky paliva může vést ke zpoždění nebo zrušení letů, což může způsobit provozní výpadky a potenciální bezpečnostní problémy, pokud se zásoby paliva kriticky sníží.

— Manipulace se systémy řízení paliva nebo měřicími zařízeními by mohla vést k plnění nesprávného množství paliva do letadla, což by ovlivnilo výpočty hmotnosti a vyvážení letadla a mohlo by způsobit incidenty související s vyčerpáním paliva.

— Neoprávněný přístup k údajům o plnění paliva by mohl umožnit aktérům hrozby manipulovat s údaji o plánování nebo zásobách paliva, což by mohlo způsobit narušení provozu letiště a dostupnosti paliva pro letadla.

Příklad 7: Systém NOTAM příslušného vnitrostátního úřadu a související infrastruktura

— **Aktiva/doména vektoru hrozby**

— infrakstruktura a digitální rozhraní vnitrostátního systému NOTAM

— dodavatelský řetězec pro údržbu a aktualizace systému NOTAM

— IT aktiva příslušného vnitrostátního úřadu používaná pro vytváření, distribuci a uložení NOTAM

— **Nevyčerpávající souhrn potenciálních hrozeb**

— hrozba (dostupnost): narušení systému NOTAM nebo jeho přístupu

— hrozba (integrita): manipulace s daty NOTAM nebo neoprávněné vytvoření NOTAM

— hrozba (důvěrnost): neoprávněný přístup k datům NOTAM

— **Souhrn scénářů hrozeb a jejich potenciálních škodlivých dopadů na bezpečnost**

  — Narušení systému NOTAM by mohlo zabránit šíření kritických leteckých informací pilotům a řídícím letového provozu, potenciálně vedoucímu k bezpečnostním problémům.

  — Manipulace s daty NOTAM nebo neoprávněné vytváření zpráv NOTAM by mohlo vést k šíření nesprávných informací, což může vést k tomu, že piloti činí rozhodnutí na základě nepravdivých nebo zavádějících údajů.

  — Neoprávněný přístup k datům NOTAM by mohl vést k úniku informac,í potenciálně odhalujícímu citlivé provozní informace.

Příklad 8: Systém příkazů k zachování letové způsobilosti (AD) leteckého úřadu a související infrastruktura

— **Aktiva/doména vektoru hrozby**

  — infrakstruktura a digitální rozhraní systému EASA AD

  — dodavatelský řetězec pro údržbu a aktualizace systému AD

  — IT aktiva EASA používaná pro vytváření, distribuci a uložení AD

— **Nevyčerpávající souhrn potenciálních hrozeb**

  — hrozba (dostupnost): narušení systému AD nebo jeho přístupu

  — hrozba (integrita): manipulace s daty AD nebo neoprávněné vytvoření AD

  — hrozba (důvěrnost): neoprávněný přístup k datům AD

— **Souhrn hrozeb a jejich potenciálních škodlivých dopadů na bezpečnost**

  — Narušení systému AD by mohlo zabránit šíření kritických informací pro letovou způbilost provozovatelům letadel a organizacím pro údržbu, potenciálně vedoucímu k bezpečnostním problémům.

  — Manipulace s daty AD nebo neoprávněné vytváření AD by mohlo vést k šíření nesprávných informací, což by mohlo vést k tomu, že provozovatelé letadel a organizace pro údržbu se rozhodují na základě nepravdivých nebo zavádějících údajů.

  — Neoprávněný přístup k datům AD by mohl vést k úniku informací, potenciálně odhalujícímu citlivé provozní informace.

Dodatek II
Hlavní úkoly vyplývající z implementace Části IS, včetně mapy vztahů kompetencí dle NIST CSF 1.1 a článků a prostředků řízení dle ISO/IEC 27001

Hlavní úkol dle Části IS	Typ činnosti	Reference					
	Řízení, Provozní	Část IS	NIST CSF verze 1.1		ISO/IEC 27001		
			Funkce	Kategorie	Ustanovení odstavce	Annex A Control	
						:2013	:2022
Vytvořit a provozovat systém řízení bezpečnosti informací (ISMS)	Řízení	IS.D.OR.200(a)	IDENTIFIKOVAT	ID.RM	4 6.1.1		
Stanovit rozsah ISMS podle požadavků Části IS	Řízení	IS.D.OR.205(a)	IDENTIFIKOVAT	ID.BE-2 ID.BE-4 ID.AM-5	4.3		
Implementovat a udržovat politiku bezpečnosti informací	Řízení	IS.D.OR.200(a)(1)	IDENTIFIKOVAT	ID.GV-1	5.2	A5.1	A5.1
Identifikovat a přezkoumat rizika bezpečnosti informací	Řízení	IS.D.OR.200(a)(2) IS.D.OR.205	IDENTIFIKOVAT	ID.GV-4 ID.RA	6.1.2 8.1 8.2		
Implementovat opatření pro řešení rizik bezpečnosti informací	Řízení	IS.D.OR.200(a)(3) IS.D.OR.210	CHRÁNIT	PR.PT	6.1.3 8.1 8.3		
Implementovat opatření k detekci událostí informační bezpečnosti a identifikovat ty, které se týkají bezpečnosti letectví	Řízení	IS.D.OR.200(a)(5) IS.D.OR.220	DETEKOVAT	DE.AE-3 DE.CM-1 DE.CM-2 DE.CM-3		A11.1.2 A12.4.1 A12.4.3 A16.1.7	A7.2 A8.15 A5.28
Implementovat opatření, která byla oznámena příslušným úřadem	Provozní	IS.D.OR.200(a)(6)			10.1	A6.1.3	A5.5
Přijmout vhodná nápravná opatření k řešení nálezů oznámených příslušným úřadem (neshod)	Obojí	IS.D.OR.200(a)(7) IS.D.OR.225			10.1	A6.1.3	A5.5

Hlavní úkol dle Části IS	Typ činnosti	Reference					
	Řízení, Provozní	Část IS	NIST CSF verze 1.1		ISO/IEC 27001		
			Funkce	Kategorie	Ustanovení odstavce	Annex A Control	
						:2013	:2022
Implementovat systém externích hlášení v oblasti bezpečnosti informací	Řízení	IS.D.OR.200(a)(8) IS.D.OR.230	REAGOVAT	RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5	7.4	A6.1.3 A16.1.2 A16.1.3	A5.5 A6.8
Sledovat dodržování tohoto nařízení a hlásit nálezy vrcholovému vedení	Provozní	IS.~~OI.R~~D.OR.200(a)(12)	IDENTIFIKOVAT	ID.GV-3	9.2	A18.2.1 A18.2.2	A5.35 A5.36
Chránit důvěrnost vyměňovaných informací	Provozní	IS.D.OR.200(a)(13)	CHRÁNIT	PR.DS-1 PR.DS-2		A8.2.2 A13.2	A5.13 A5.14
Implementovat a udržovat proces neustálého zlepšování pro měření účelnosti a vyspělosti ISMS a usilovat o jeho zlepšování	Řízení	IS.D.OR.200(b) IS.D.OR.260	IDENTIFIKOVAT	ID.RA-6 ID.SC-4	4.4 9.1 9.3 10.1 10.2	A5.1.2 A16.1.7 A17.1.3 A18.2.1	A5.1 A5.28 A5.29 A5.35
			CHRÁNIT	PR.IP-7 PR.IP-10			
			DETEKOVAT	DE.DP-5			
			REAGOVAT	RS.MI-3 RS.IM-2			
			OBNOVIT	RC.IM-2			
Dokumentovat a udržovat všechny klíčové procesy, postupy, role a odpovědnosti	Řízení	IS.D.OR.200(c)	IDENTIFIKOVAT	ID.AM-6 ID.GV-4 ID.RM-1 ID.SC-1 ID.SC-2	4.2 5.2 5.3	A5.1 A6.1.1	A5.1 A5.2
			CHRÁNIT	PR.AT-2 PR.AT-4 PR.AT-5 PR.IP-12			
			DETEKOVAT	DE.DP-1			
			REAGOVAT	RS.CO-1 RS.AN-5			

Hlavní úkol dle Části IS	Typ činnosti	Reference					
	Řízení, Provozní	Část IS	NIST CSF verze 1.1		ISO/IEC 27001		
			Funkce	Kategorie	Ustanovení odstavce	Annex A Control	
						:2013	:2022
Identifikovat všechny prvky, které by mohly být vystaveny rizikům bezpečnosti informací	Řízení	IS.D.OR.205(a)	IDENTIFIKOVAT	ID.AM-1 ID.AM-2 ID.AM-4 ID.AM-5	4.3	A8.1.1	A5.9
Identifikovat rozhraní s jinými organizacemi, která by mohla vést k vystavení se rizikům bezpečnosti informací	Řízení	IS.D.OR.205(b)	IDENTIFIKOVAT	ID.BE-1 ID.BE-2 ID.BE-4 ID.BE-5	4.3		
Identifikovat rizika bezpečnosti informací a přiřadit úroveň rizika	Řízení	IS.D.OR.205(c)	IDENTIFIKOVAT	ID.RA-1 ID.RA-2 ID.RA-3 ID.RA-4 ID.RA-5	6.1.2		
Přezkoumat a aktualizovat posouzení rizik na základě určitých kritérií	Provozní	IS.D.OR.205(d)	IDENTIFIKOVAT	ID.RM	8.2		A5.7
Vypracovat a implementovat opatření k řešení rizik a ověřit jejich účelnosti	Provozní	IS.D.OR.210(a)	CHRÁNIT	PR.IP PR.PT	6.1.3 8.3		
Sdělit výsledek posouzení rizik vedení, ostatnímu personálu a dalším organizacím sdílejícím rozhraní	Provozní	IS.D.OR.210(b)	IDENTIFIKOVAT	ID.AM-3 ID.BE-1 ID.BE-2 ID.BE-4 ID.RM-3 ID.SC-3	8.1		
			CHRÁNIT	PR.IP-7			
Vytvořit systém interních hlášení v oblasti bezpečnosti informací, který umožní shromažďovat a vyhodnocovat události v oblasti bezpečnosti	Řízení	IS.D.OR.200(a)(4) IS.D.OR.215(a) IS.D.OR.215(e)	IDENTIFIKOVAT	ID.AM-3	7.4	A16.1.1 A16.1.2	A5.28 A6.8

Hlavní úkol dle Části IS	Typ činnosti	Reference					
	Řízení, Provozní	Část IS	NIST CSF verze 1.1		ISO/IEC 27001		
			Funkce	Kategorie	Ustanovení odstavce	Annex A Control	
						:2013	:2022
informací od personálu							
Zajistit, aby smluvní organizace hlásily události v oblasti bezpečnosti informací	Řízení	IS.D.OR.215(c)	REAGOVAT	RS.CO-2 RS.CO-4	7.4	A15.1.1 A16.1.2	A5.19 A6.8
Analyzovat interně hlášené události s cílem identifikovat události, incidenty a zranitelnosti v oblasti bezpečnosti informací	Provozní	IS.D.OR.215(b)(1)–(b)(3)	IDENTIFIKOVAT	ID.RA-1		A12.6.1 A16.1.1 A16.1.4	A8.8 A5.24 A5.25
			DETEKOVAT	DE.AE-2 DE.AE-3 DE.AE-5			
Implementovat opatření k detekci událostí v oblasti bezpečosti informací v procesech a provozu, které mohou mít potenciální dopad na bezpečnost letectví	Provozní	IS.D.OR.220(a)	DETEKOVAT	DE.AE DE.CM DE.DP		A11.1.2 A12.4.1 A12.6.1 A16.1.1 A16.1.2 A16.1.3 A16.1.4 A16.1.5	A7.2 A8.8 A8.15 A8.16 A5.24 A5.25 A5.26 A6.8
			CHRÁNIT	PR.PT-1			
Implementovat opatření k reakci na události bezpečnosti informací, které mohou způsobit incident v oblasti bezpečnosti informací	Provozní	IS.D.OR.220(b)	REAGOVAT	RS.RP RS.AN RS.MI		A16.1.5	A5.26
Spolupracovat na vyšetřování s dalšími organizacemi, které se podílejí na bezpečnosti informací jeho vlastních činností	Řízení	IS.D.OR.215(d)	REAGOVAT	RS.AN-3 RS.AN-5		A15.1.2 A15.1.3 A16.1.7	A5.20 A5.21 A5.28
Implementovat opatření k zotavení se	Provozní	IS.D.OR.220(c)	OBNOVIT	RC.RP-1 RC.IM-1		A16.1.5 A16.1.6	A5.26 A5.27

Hlavní úkol dle Části IS	Typ činnosti	Reference					
	Řízení, Provozní	Část IS	NIST CSF verze 1.1		ISO/IEC 27001		
			Funkce	Kategorie	Ustanovení odstavce	Annex A Control	
						:2013	:2022
(obnově) z incidentů v oblasti bezpečnosti informací							
Řídit rizika spojená se smluvními činnostmi s ohledem na řízení bezpečnosti informací	Řízení	IS.D.OR.235	IDENTIFIKOVAT	ID.SC-1 ID.SC-2		A15.1 A15.2	A5.19 A5.20 A5.21 A5.22
Vytvořit a udržovat proces, který zajistí, že bude k dispozici dostatek personálu pro provádění všech činností týkajících se řízení bezpečnosti informací	Řízení	IS.D.OR.240(f)	IDENTIFIKOVAT	ID.AM-5 ID.AM-6 ID.GV-2	7.1	A6.1.1	A5.2
Vytvořit a udržovat proces, který zajistí, že personál bude mít nezbytnou způsobilost (kompetenci) pro činnosti týkající se řízení bezpečnosti informací	Řízení	IS.D.OR.240(g)	IDENTIFIKOVAT CHRÁNIT	ID.AM-5 ID.AM-6 PR.AT-1	7.2	A7.2.2	A6.3
Vytvořit a udržovat proces, který zajistí, že personál uznává odpovědnosti spojené s přidělenými rolemi a úkoly	Řízení	IS.D.OR.240(h)	IDENTIFIKOVAT	ID.GV-2 ID.GV-3	7.3 7.4	A7.1.2	A6.2
Ověřovat identitu a důvěryhodnost personálu, který má přístup k informačním systémům	Řízení	IS.D.OR.240(i)	CHRÁNIT	PR.AC-6 PR.IP-11	7.1	A7.1.1	A6.1
	Provozní	IS.D.OR.245	IDENTIFIKOVAT	ID.RA-4	7.5		

Hlavní úkol dle Části IS	Typ činnosti	Reference					
	Řízení, Provozní	Část IS	NIST CSF verze 1.1		ISO/IEC 27001		
			Funkce	Kategorie	Ustanovení odstavce	Annex A Control	
						:2013	:2022
Archivovat, chránit a uchovávat záznamy a zajistit, že jsou vysledovatelné po stanovenou dobu			CHRÁNIT	PR.AC-2 PR.AC-3 PR.AC-4 PR.DS-1 PR.DS-4 PR.DS-5 PR.DS-6 PR.IP-4 PR.IP-6 PR.PT-1		A8.2.2 A8.2.3 A11.1.3 A11.1.4 A12.1.3 A12.3.1 A12.4.1 A12.4.2 A12.4.3	A5.10 A5.13 A7.3 A7.5 A8.6 A8.10 A8.13 A8.15
Provést nápravu nálezů neshod na základě oznámení příslušného úřadu ve lhůtě dohodnuté s příslušným úřadem	Provozní	IS.D.OR.225			10.1	A18.1.1 A18.2	A5.31 A5.35 A5.36
Implementovat systém hlášení v oblasti bezpečnosti informací v souladu s nařízením (EU) č. 376/2014	Řízení	IS.D.OR.230(a)					
Hlásit incidenty nebo zranitelnosti bezpečnosti informací příslušnému úřadu a za určitých podmínek i ostatním	Provozní	IS.D.OR.230(b) IS.D.OR.230(c)	DETEKOVAT	DE.DP-3	7.4	A16.1.1 A16.1.2 A16.1.3	A5.24 A6.8
			REAGOVAT	RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5			
			OBNOVIT	RC.CO-3			
Pravidelně posuzovat účelnost a vyspělost ISMS	Provozní	IS.D.OR.260(a)			9	A5.1.2 A12.7.1 A16.1.6	A5.1 A5.27 A8.34
V případě potřeby podniknout kroky ke zlepšení ISMS. Opětovně posoudit prvky ISMS ovlivněné implementovanými opatřeními.	Provozní	IS.D.OR.260(b)			10	A5.1.2	A5.1

Hlavní úkol dle Části IS	Typ činnosti	Reference					
	Řízení, Provozní	Část IS	NIST CSF verze 1.1		ISO/IEC 27001		
			Funkce	Kategorie	Ustanovení odstavce	Annex A Control	
						:2013	:2022
Zajistit příslušnému úřadu přístup ke smluvní organizaci	Řízení	IS.D.OR.235(b)			9.3	A6.1.3 A15.1 A15.2	A5.5 A5.20 A5.22
Vrcholové vedení zajistí, aby byly k dispozici veškeré zdroje nezbytné ke splnění tohoto nařízení	Řízení	IS.D.OR.240(a)(1)	IDENTIFIKOVAT	ID.AM-5 ID.AM-6	7.1	A6.1.1	A5.2
Vrcholové vedení zavede a podporuje politiku bezpečnosti informací a prokazuje základní porozumění tomuto nařízení	Řízení	IS.D.OR.240(a)(2) &(a)(3)	IDENTIFIKOVAT	ID.GV-1	5.1 5.2 7.4	A5.1.1 A7.2.1 A7.2.2	A5.1 A5.4 A6.3
			CHRÁNIT	PR.AT-1 PR.AT-4			
Jmenovat odpovědnou osobu nebo skupinu osob s příslušnými znalostmi k řízení souladu s tímto nařízením	Řízení	IS.D.OR.240(b) IS.D.OR.240(c) IS.D.OR.240(d)	IDENTIFIKOVAT	ID.AM-6 ID.GV-2	7.1 7.2	A6.1.1 A7.2.1 A7.2.2	A5.2 A5.4 A6.3
			CHRÁNIT	PR.AT-1 PR.AT-4			
Vytvořit a udržovat příručku pro řízení bezpečnosti informací (ISMM)	Řízení	IS.D.OR.250			7.5.1	A6.1.3 A12.1.1	A5.5 A5.37
Vypracovat postup, jak příslušnému úřadu oznamovat změny ISMS	Řízení	IS.D.OR.255(a)	IDENTIFIKOVAT	ID.AM-3	7.4 7.5.1	A6.1.3 A13.2.1 A13.2.2	A5.5 A5.14
Řídit změny ISMS a oznamovat příslušnému úřadu změny a/nebo požádat o jejich schválení	Řízení	IS.D.OR.255(a) IS.D.OR.255(b)	IDENTIFIKOVAT	ID.AM-3	7.4	A6.1.3 A13.2.1 A13.2.2	A5.5 A5.14

Dodatek III
Příklady leteckých služeb

Níže je uveden nevyčerpávající a neúplný seznam leteckých služeb, které lze použít jako základ pro identifikaci rozsahu posuzování rizik pro organizaci.

poskytovatel letištních ATM-MET služeb
služba letecké digitální mapy
AIM (externí)
letiště
APP ACC
ATC (externí)
ATC superior
ATM
poskytovatel služeb ATM-MET
operační středisko civilních AU (uživatelů vzdušného prostoru)
komunikační infrastruktura
ER ACC
integrátor dat FIS/TIS
národní AIM
navigační infrastruktura – pozemní
navigační infrastruktura – družicová
poskytovatel služeb jiných než ATM-MET
neletečtí uživatelé (externí)
regionální AIM
regionální ASM
regionální ATFCM
operační středisko státních AU (uživatelů vzdušného prostoru)
služba statických leteckých dat
poskytování společné subregionální služby DCB
subregionální/místní ATFCM

subregionální/národní ASM
přehledová infrastruktura letištní
přehledová infrastruktura traťová
přehledová infrastruktura TMA
časová reference (externí)
věž (TWR)

Přijatelné způsoby průkazu a poradenský materiál k Příloze II (Část IS.I.OR) k prováděcímu nařízení Komise (EU) 2023/203

První vydání

12. července 2023[1]

[1] Datum vstupu v platnost tohoto vydání prosím viz rozhodnutí 2023/009/R v Úřední publikaci EASA.

OBSAH

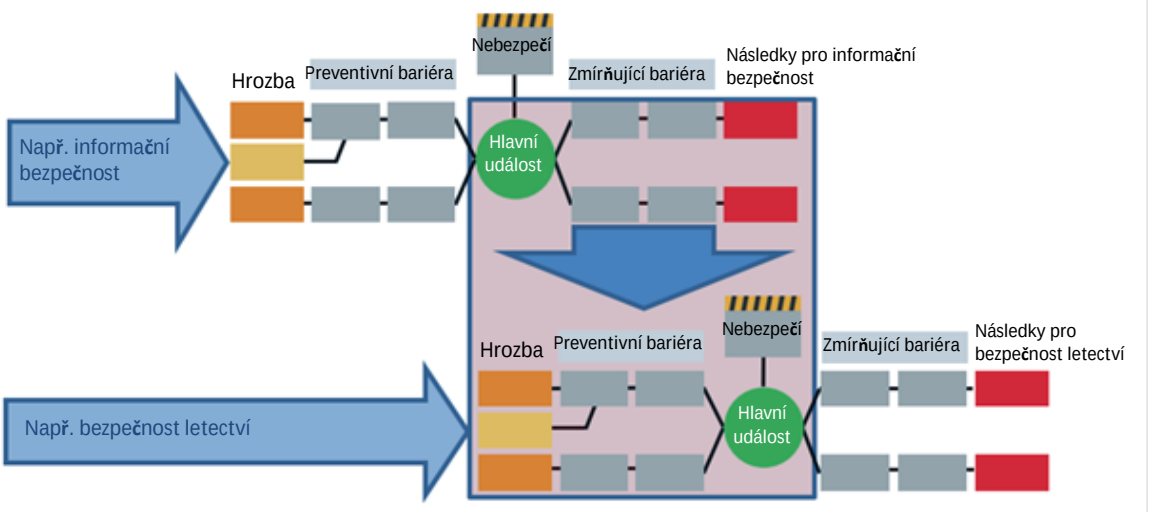
AMC A GM K PŘÍLOZE II (ČÁST IS.I.OR) K PROVÁDĚCÍMU NAŘÍZENÍ KOMISE (EU) 2023/203

GM1 IS.I.OR.200 Systém řízení bezpečnosti informací (ISMS)

Systém řízení bezpečnosti informací (ISMS) je systematický přístup k ustavení, implementaci, provádění, monitorování, přezkoumávání, udržování a neustálému zlepšování stavu informační bezpečnosti v rámci organizace. Jeho cílem je chránit informační aktiva tak, aby provozních a bezpečnostních cílů organizace bylo možné dosáhnout s vědomím rizik, účinným a efektivním způsobem.

Obecně řečeno, ISMS zavádí proces řízení rizik v oblasti bezpečnosti informací, na základě výsledků analýz dopadů v oblasti bezpečnosti informací, které v podstatě určují jeho rozsah. Pokud narušení bezpečnosti informací může způsobit následky pro bezpečnost letectví nebo k nim přispět, musí požadavky na zabezpečení informací omezit jejich vliv na úrovně bezpečnosti letectví, které jsou považovány za přijatelné. Všechny role, procesy nebo informační systémy, které mohou způsobit následky pro bezpečnost letectví nebo k nim přispět, tedy spadají do oblasti působnosti nařízení (EU) 2023/203. ISMS poskytuje způsob, jak rozhodnout o potřebných opatřeních v oblasti informační bezpečnosti pro všechny architektonické vrstvy (správa a řízení, obchod, aplikace, technologie, data) a domény (organizační, lidská, fyzická, technická). Dále umožňuje řídit výběr, implementaci a provádění opatření v oblasti informační bezpečnosti. Konečně umožňuje řídit správu a řízení, řízení rizik a shodu (GRC) v rámci ISMS.

Proces řízení rizik je tedy založen na posuzováních rizik bezpečnosti letectví a odvozených úrovních přijatelnosti rizik v oblasti bezpečnosti informací, které jsou navrženy tak, aby účinně ošetřovaly a řídily rizika v oblasti bezpečnosti informací s potenciálním dopadem na bezpečnost letectví způsobená hrozbami využívajícími zranitelností informačních aktiv v leteckých systémech. Interagující motýlkové *(bow-tie)* diagramy umožňují ilustraci (na vyšší úrovni a nevyčerpávající) toho, jak může být nezbytné, aby různé obory posuzování rizika spolupracovaly, s cílem vytvořit společnou perspektivu na riziko, jak je znázorněno na obrázku 1.



Obrázek 1: Zobrazení řízení rizik v oblasti bezpečnosti letectví, která představují hrozby informační bezpečnosti, prostřednictvím motýlkového diagramu

ISMS v tomto nařízení by měl spojovat kompetence v oblasti bezpečnosti informací a bezpečnosti letectví ve většině procesů, včetně například identifikace kritických systémů nebo hrozeb a posuzování potenciálních dopadů na bezpečnost letectví a rizik pro něj.

Implementace a udržování ISMS

ISMS, jak je definován v tomto nařízení, využívá perspektivy správy a řízení, rizika a shody a přístup, který kombinuje dimenze bezpečnostního rizika a výkonnosti, aby určil opatření v oblasti bezpečnosti informací, které jsou vhodné a v souladu s konkrétním kontextem a mohou účinně poskytovat úroveň ochrany požadovanou k dosažení cílů v oblasti bezpečnosti letectví prostřednictvím:

— Hledisko **správy a řízení** se týká poskytování směru a vedení managementu s cílem dosáhnout vlastních zastřešujících cílů subjektu:

  — vedení a závazek vrcholového managementu definující a zajišťující úzké zapojení managementu a implementaci ISMS „shora dolů“

  — cíle bezpečnosti informací a bezpečnosti v souladu a konzistentní s obchodními cíli subjektu a monitorované např. přezkoumáními managementem

  — politiky informační bezpečnosti stanovující zásady a cíle, kterých má být dosaženo

  — role, odpovědnosti, kompetence a zdroje potřebné pro efektivní ISMS

  — efektivní, na cílovou skupinu orientovaná komunikace s interními a externími zainteresovanými stranami

— Hledisko **rizik** odkazuje na klíčový aspekt ISMS v kontextu bezpečnosti letectví podle tohoto nařízení a slouží jako základ pro transparentní rozhodování a stanovení priorit kontrol a možností řešení rizik. Dále se týká posuzování, řešení a monitorování rizik informační bezpečnosti na podporu řízení rizik v oblasti bezpečnosti letectví pro klíčové procesy a informační aktiva, na kterých závisí. To zahrnuje požadavky na ochranu, vystavení riziku, postoj k rizikům a kritéria přijatelnosti rizik, metody a průmyslové normy.

— Hledisko **shody** se týká souladu s regulačními, právními a smluvními požadavky. To zahrnuje:

  — toto nařízení,

  — vlastní zásady a normy subjektu a dále mohou zahrnovat mezinárodní nebo průmyslové normy převzaté subjektem od ISO, EUROCAE atd.

  Toto hledisko zahrnuje definici, implementaci a udržování požadovaných ustanovení o bezpečnosti informací, jejichž účelnost a soulad by měly být pravidelně sledovány a zajišťovány např. (interními) audity.

Na základě těchto hledisek můžeme identifikovat následující procesy a předmětové oblasti, které se ukázaly jako relevantní pro zavedení efektivního ISMS. Tyto procesy a oblasti ISMS lze shrnout takto:

(a) vytvoření kontextu definujícího rozsah, rozhraní, závislosti a požadavky zainteresovaných stran;

(b) vedení a závazek vrcholového managementu;

(c) cíle informační bezpečnosti a bezpečnosti;

(d) zásady v oblasti bezpečnosti informací;

(e) role, odpovědnosti, kompetence a zdroje potřebné pro efektivní;

(f) komunikace s interními a externími zainteresovanými stranami k dosažení dostatečné úrovně povědomí v oblasti bezpečnosti informací a školení všech zúčastněných stran;

(g) řízení rizik v oblasti bezpečnosti informací včetně posuzování a řešení rizik;

(h) řízení incidentů bezpečnosti informací zavádějící procesy pro zvládání incidentů a zranitelností v oblasti bezpečnosti informací;

(i) monitorování, měření a vyhodnocování výkonnosti a účelnosti;

(j) interní audity a přezkoumání managementem;

(k) nápravy a nápravná opatření;

(l) neustálé zlepšování;

(m) vztah s dodavateli;

(n) dokumentace, vedení záznamů a shromažďování důkazů.

Mezi další kritické faktory úspěchu pro implementaci a provádění ISMS patří:

— ISMS by měl být integrován do procesů subjektu a celkové struktury řízení nebo dokonce – alespoň částečně, se zárukami pro jejich příslušnou integritu, a pokud je to rozumně aplikovatelné – se zastřešujícím systémem řízení zahrnujícím informační bezpečnost, bezpečnost letectví a řízení kvality.

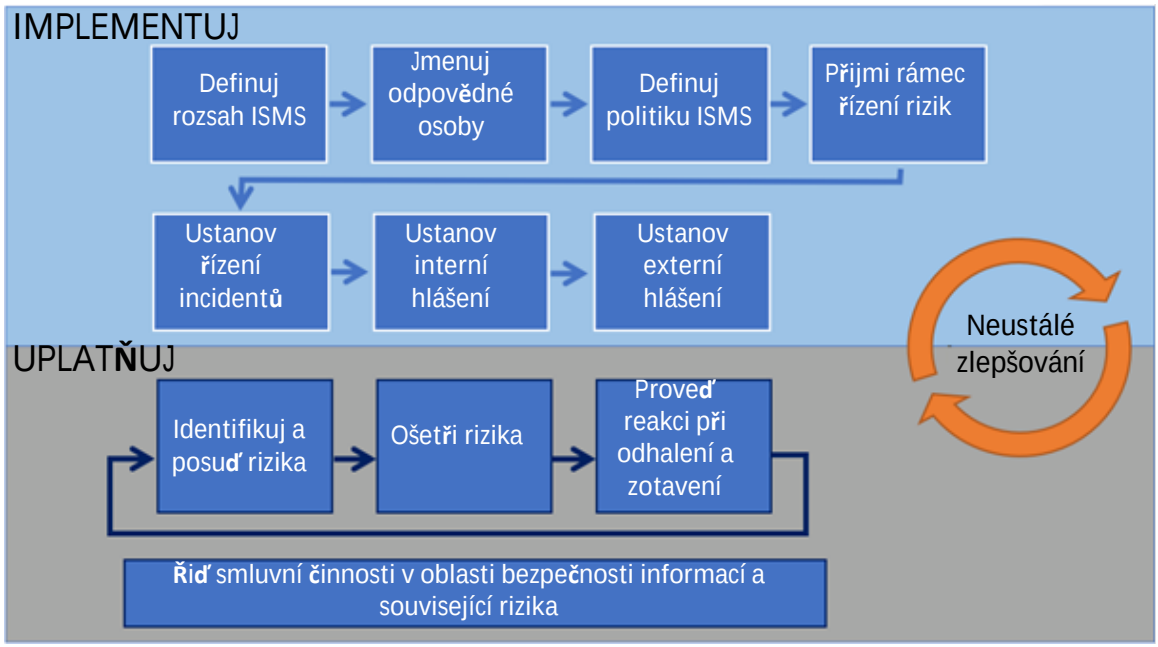
— Informační bezpečnost musí být zohledněna v rané fázi celkového návrhu procesů a postupů, systémů a opatřeních v oblasti informační bezpečnosti, aby byly hladce integrovány, aby byla zajištěna maximální účelnost, minimální funkční interference a optimalizované náklady. Žádného z těchto přínosů nelze dosáhnout pozdější integrací.

— Proces řízení rizik určuje vhodné charakteristiky preventivních opatření pro dosažení a udržení přijatelných úrovní rizik.

— Proces řízení incidentů zajišťuje, že organizace včas odhalí, reaguje a odpovídá na incidenty v oblasti informační bezpečnosti. Toho je dosaženo tím, že se předem definují odpovědnosti, postupy, scénáře a plány reakce, aby byla zajištěna koordinovaná, cílená a účinná reakce.

— Provádí se průběžné monitorování a přehodnocování a v reakci na to jsou prováděna zlepšení.

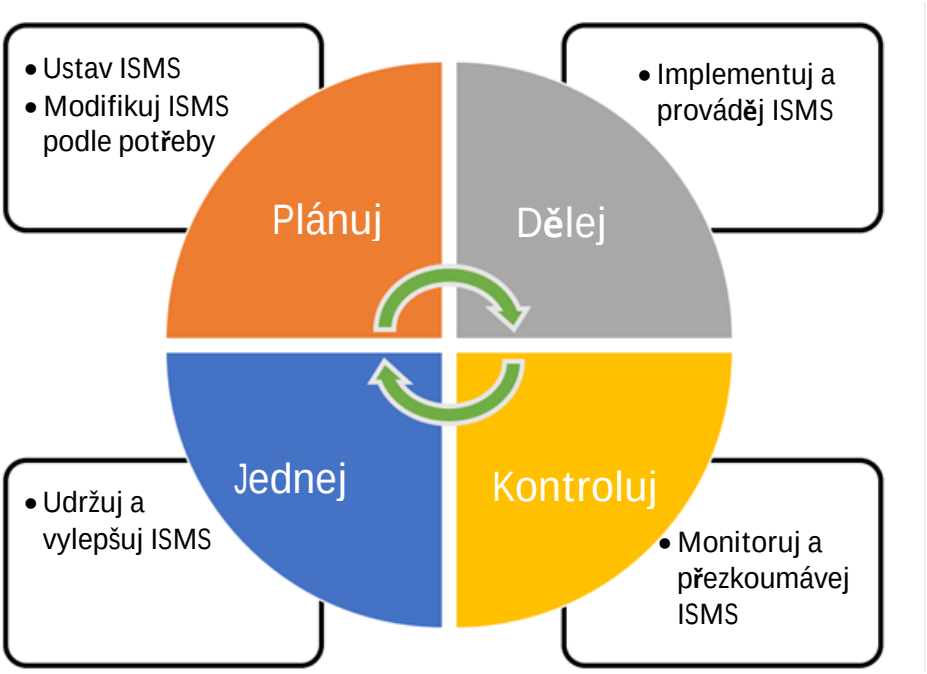
Výše uvedené základní komponenty souvisejí s požadavky tohoto nařízení, pro které obrázek 2 poskytuje zobrazení aspektů na vysoké úrovni, které jsou významnější ve fázi implementace, a těch, které charakterizují provozní fázi, jakož i přezkum a možné zlepšení, pokud funkce nefungují podle plánu.



Obrázek 2: Zobrazení požadavků Části IS z pohledu životního cyklu ISMS

Přístup plánuj-dělej-kontroluj-jednej (PDCA)

PDCA *(Plan-Do-Check-Act)* označuje procesní přístup, který se často používá k vytvoření, implementaci, uplatňování, monitorování, přezkoumávání a zlepšování systémů řízení. Obrázek 3 znázorňuje PDCA aplikovaný na ISMS.



Obrázek 3: Přístup PDCA aplikovaný na ISMS

Přínosy ISMS

Přínosy systému řízení fungujícího v dynamickém, nejistém nebo nepředvídatelném prostředí rizik se v dlouhodobém horizontu projeví pouze tehdy, když organizace zlepší stávající opatření, procesy a řešení na základě posuzování rizik, výkonnosti a vyspělosti, jakož i poučení z incidentů, auditů, neshod a jejich kořenových příčin. Úspěšné přijetí a nasazení ISMS umožňuje subjektu:

— dosáhnout větší jistoty pro management a zainteresované strany, že jejich informační aktiva jsou neustále přiměřeně chráněna proti hrozbám;

— zvýšit svou důvěryhodnost a hodnověrnost poskytnutím důvěry zainteresovaným stranám, že rizika v oblasti bezpečnosti informací s dopadem na bezpečnost letectví jsou náležitě řízena;

— zvýšit odolnost klíčových procesů subjektu proti neoprávněným elektronickým interakcím a zachovat schopnost subjektu rozhodovat a jednat;

— podporovat včasné odhalování mezer v opatřeních, zranitelností nebo nedostatků s cílem předcházet incidentům v oblasti informační bezpečnosti nebo alespoň minimalizovat jejich dopad;

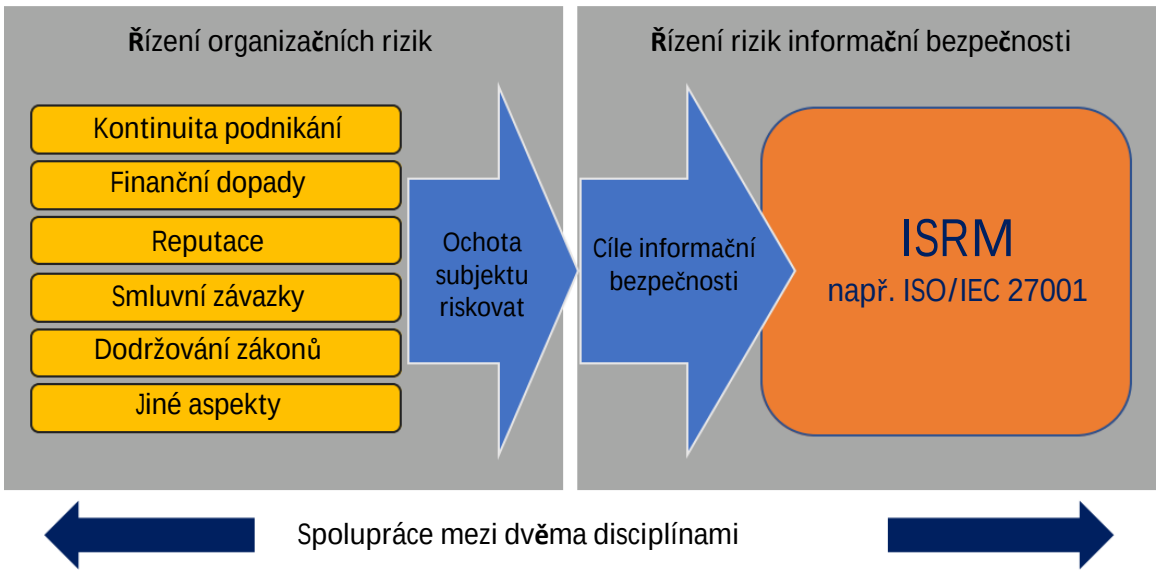
— detekovat a včas reagovat na změny v prostředí subjektu, včetně architektury systému a prostředí hrozeb nebo přijetí nových technologií;

— poskytnout základ pro efektivní a účinnou implementaci komplexní strategie v oblasti informační bezpečnosti v době digitální transformace, rostoucí interkonektivity systémů, vznikajících hrozeb v oblasti informační bezpečnosti a nových technologií.

Vztak k normě ISO/IEC 27001

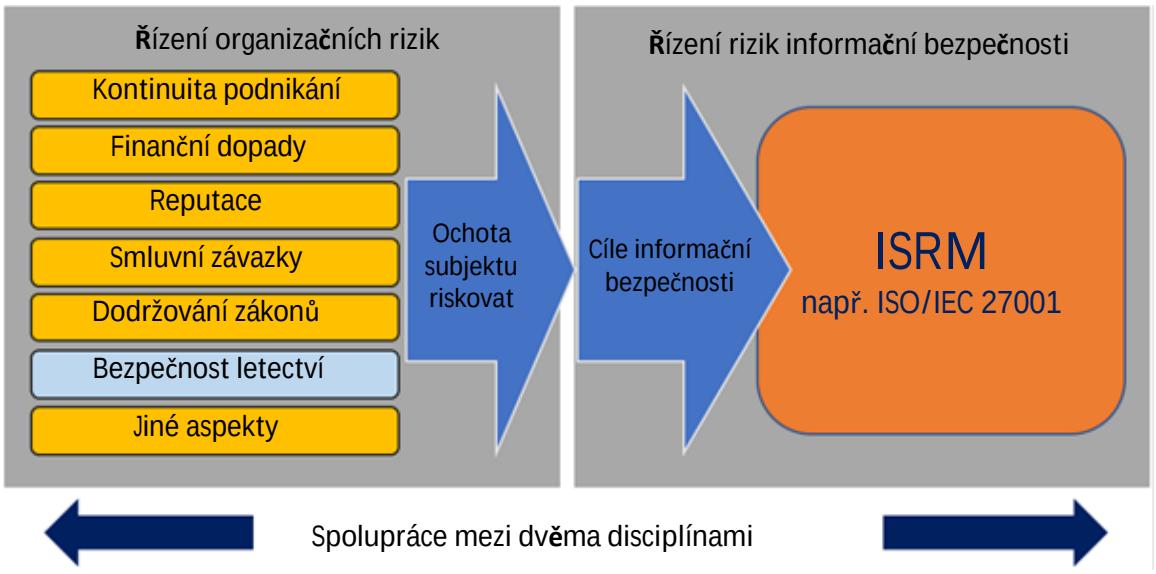
Mezinárodní norma ISO/IEC 27001 je široce přijímaná norma pro ISMS, která specifikuje obecné požadavky na ustavení, implementaci, udržování a neustálé zlepšování ISMS. Zahrnuje také požadavky na posuzování a řešení rizik informační bezpečnosti. Požadavky se vztahují na všechny subjekty bez ohledu na typ, velikost nebo povahu. Shoda ISMS s normou ISO/IEC 27001 může být certifikována akreditovaným certifikačním orgánem. ISO/IEC 27001 je kompatibilní s jinými normami systému řízení (kvality, bezpečnosti atd.), které také přijaly strukturu a termíny definované v příloze Annex SL to ISO/IEC Directives, Part 1, Consolidated ISO Supplement. Tato kompatibilita umožňuje subjektu provozovat jeden systém řízení, který splňuje požadavky více standardů systému řízení.

ISO/IEC 27001 umožňuje subjektům definovat vlastní rozsah auditu a vlastní ochotu organizace riskovat. To zase vede k požadavkům na bezpečnost informací, které poskytují ISMS kritéria přijatelnosti rizik informační bezpečnosti v souladu s ochotou subjektu riskovat (viz obrázek 4).



Obrázek 4: Vztah mezi ochotou subjektu riskovat a cíli informační bezpečnosti

Požadavky na ISMS specifikované tímto nařízením jsou ve většině částí konzistentní a v souladu s ISO/IEC 27001; toto nařízení však zavádí ustanovení specifická v kontextu bezpečnosti letectví. Pokud ISMS založený na ISO/IEC 27001 již subjekt provozuje pro jiný rozsah a kontext, lze jej upravit a rozšířit na oblast působnosti a kontextu tohoto nařízení jednoduchým způsobem na základě analýzy rozsahu a nedostatků. Aby bylo možné získat kredit z certifikací ISO/IEC 27001 za účelem dosažení souladu s Částí IS, musí být bezpečnost letectví zahrnuta do řízení rizik organizace s příslušnou úrovní přijatelnosti rizik stanovenou příslušným předpisem (viz obrázek 5). Proto je nutné pečlivé stanovení rozsahu ISMS v souvislosti s riziky v obůasti bezpečnosti letectví, protože se může lišit od rozsahu ve spojitosti s ostatními organizačními riziky. Aby bylo možné prokázat shodu s nařízením (EU) 2023/203, může být nutné pečlivé vymezení aspektů ISMS v souvislosti s riziky v oblasti bezpečnosti letectví a dalšími organizačními riziky. To by mohlo mít vliv na rozhodnutí o integraci ISMS.



Obrázek 5: Začlenění aspektů bezpečnosti letectví do ochoty subjektu riskovat

ČÁST IS versus ISO/IEC 27001 – tabulka křížových odkazů

Mapu vztahů mezi hlavními úkoly požadovanými podle Části IS a články a souvisejícími prostředky řízení v ISO/IEC 27001 naleznete v Dodatku II.

AMC1 IS.I.OR.200(a)(1) Systém řízení bezpečnosti informací

Organizace by měla definovat a zdokumentovat rozsah ISMS stanovením činností, procesů, podpůrných systémů a určením těch, které mohou mít dopad na bezpečnost letectví.

Politika bezpečnosti informací by měla být schválena odpovědným vedoucím a přezkoumávána v plánovaných intervalech, nebo pokud dojde k významným změnám. Kromě toho by politika měla zahrnovat alespoň následující aspekty s potenciálním dopadem na bezpečnost letectví:

(a) zavázat se dodržovat platnou legislativu, zvážit příslušné normy a osvědčené postupy;

(b) stanovit cíle a výkonnostní opatření pro řízení informační bezpečnosti;

(c) definovat obecné zásady, činnosti, procesy pro organizaci za účelem náležitého zabezpečení systémů a dat informačních a komunikačních technologií;

(d) zavázat se aplikovat požadavky ISMS do procesů organizace;

(e) zavázat se neustále se zlepšovat směrem k vyšším úrovním vyspělosti procesu zabezpečení informací podle IS.I.OR.260;

(f) zavázat se plnit platné požadavky týkající se informační bezpečnosti a jejího proaktivního a systematického řízení a poskytovat odpovídající zdroje pro jeho implementaci a fungování;

(g) určit informační bezpečnost jako jednu ze základních povinností všech manažerů;

(h) zavázat se pravidelně nebo po modifikacích podporovat politiku bezpečnosti informací prostřednictvím školení nebo osvětových setkání pro všechny zaměstnance v rámci organizace;

(i) podporovat zavádění kultury „spravedlivého posuzování *(just culture)*“ a hlášení zranitelností, podezřelých/anomálních událostí a/nebo incidentů v oblasti bezpečnosti informací;

(j) zavázat se sdělit politiku bezpečnosti informací podle potřeby všem relevantním stranám.

Poznámka: Významná změna je výrazná změna nebo modifikace, která má významný dopad na fungování organizace, jako je strukturální změna v rámci organizace v důsledku reorganizací, změna ve firemních procesech (např. práce z domova, používání osobních zařízení), technologický vývoj (např. distribuované výpočetní zdroje, umělá inteligence/strojové učení) nebo vývoj v oblasti hrozeb.

GM1 IS.I.OR.200(a)(1) Systém řízení bezpečnosti informací (ISMS)

POLITIKA A CÍLE V OBLASTI BEZPEČNOSTI INFORMACÍ

Politika bezpečnosti informací by měla vyhovovat účelu příslušného úřadu a řídit jeho vlastní činnosti v oblasti bezpečnosti informací. Taková politika by měla obsahovat potřeby bezpečnosti informací v kontextu dané organizace, prohlášení na vysoké úrovni o směru a záměru činností v oblasti bezpečnosti informací, zásady a nejdůležitější strategické a taktické cíle, kterých má být prostřednictvím ISMS dosaženo, a také obecné cíle informační bezpečnosti nebo specifikace rámce (kdo, jak) pro stanovení cílů informační bezpečnosti. Politika informační bezpečnosti by také měla obsahovat popis stanoveného ISMS, včetně rolí, odpovědností a odkazů na politiky a standardy specifické pro dané téma.

Cíle informační bezpečnosti by měly být:

— konzistentní a v souladu s politikou informační bezpečnosti a měly by brát v úvahu použitelné požadavky na informační bezpečnost, odvozené od zastřešujících cílů organizace, a výsledky z posuzování a řešení rizik (což naopak podporuje implementaci strategických cílů organizace a politiky informační bezpečnosti);

— pravidelně přezkoumávány, aby bylo zajištěno, že jsou aktuální a stále vhodné;

— měřitelné, pokud je to možné (aby bylo možné určit, zda byl cíl splněn), měly by být SMART (konkrétní *(specific)*, měřitelné *(measurable)*, dosažitelné *(attainable)*, realistické *(realistic)*, časově ukotvené *(timely)*) a spojeny se všemi dotčenými odpovědnými osobami.

Při definování cílů informační bezpečnosti, např. na základě zastřešujících cílů organizace, požadavků na bezpečnost informací nebo výsledků posuzování rizik, by se mělo určit, jak bude těchto cílů dosaženo. Do jaké míry je cílů informační bezpečnosti dosaženo, musí být měřitelné. Pokud je to možné, měla by být měřena pomocí klíčových ukazatelů výkonnosti (KPI), které byly definovány předem (viz zdroje, jako je COBIT 5 pro informační bezpečnost). Doporučuje se začít s definicí omezeného počtu cílů informační bezpečnosti, které jsou pro danou organizaci relevantní, mají spíše dlouhodobý charakter a jsou měřitelné s vynaložením přiměřeného úsilí ve vztahu k dosaženým přínosům.

AMC1 IS.I.OR.200(a)(12) Systém řízení bezpečnosti informací (ISMS)

SLEDOVÁNÍ SHODY

Při zjišťování shody s ustanoveními podle bodů IS.I.OR.200(a)(12) by měla organizace zavést funkci pro pravidelné sledování shody systému řízení s příslušnými požadavky a přiměřenosti postupů, včetně zřízení procesu interního auditu a procesu řízení rizik v oblasti bezpečnosti informací. Pokud již organizace zavedla funkci sledování shody podle prováděcího nařízení pro svou doménu, měla by tato funkce zahrnovat sledování systému řízení s příslušnými požadavky v rámci rozsahu jejích činností. Sledování shody by mělo zahrnovat mechanismus zpětné vazby k nálezům auditu odpovědnému vedoucímu nebo delegované osobě (delegovaným osobám), aby se zajistilo provedení nápravných opatření, pokud je to nutné.

GM1 IS.I.OR.200(a)(12) Systém řízení bezpečnosti informací (ISMS)

SLEDOVÁNÍ SHODY

Pro účely sledování shody by měly být prováděny interní audity v plánovaných intervalech, aby se vedení ujistilo o stavu ISMS a poskytly informace o následujícím:

— souladu ISMS s požadavky tohoto nařízení a vlastními požadavky organizace buď uvedenými v politice, postupech a smlouvách v oblasti bezpečnosti informací nebo odvozených z cílů informační bezpečnosti nebo výsledků procesu řešení rizik;

— efektivní implementaci a udržování ISMS.

Interní audity by se měly řídit nezávislým přístupem a rozhodovacím procesem založeným na důkazech. Kromě toho by při sestavování programu auditu měla být zvážena důležitost příslušných procesů a definice kritérií a rozsahu auditu. Měly by být uchovávány zdokumentované informace dokládající výsledky auditu, jejich hlášení příslušnému vedení a program auditu.

AMC1 IS.I.OR.200(a)(13) Systém řízení bezpečnosti informací (ISMS)

Při zjišťování shody s ustanoveními podle bodu IS.I.OR.200(a)(13) by měla organizace zavést a udržovat opatření v oblasti bezpečnosti informací, která jsou dostatečně robustní a účinná, aby chránila informace a zajistila zásadu „potřeba vědět“ (tj. omezení přístupu k informacím pouze na ty, kteří je potřebují k plnění svých povinností). Měl by chránit zdroj informací v souladu s příslušnými ustanoveními stanovenými v nařízení (EU) 2018/1139. Měl by být také v souladu s nařízením (EU) č. 376/2014.

AMC1 IS.I.OR.200(c) Systém řízení bezpečnosti informací (ISMS)

Při zjišťování shody s ustanoveními bodu IS.I.OR.200(c) by organizace měla:

(a) poskytnout přehled struktury konkrétního personálu v oblasti bezpečnosti informací (interního a externího), včetně jejich rolí a odpovědností. Tento přehled bude použit pro řízení a udržování prvků zahrnutých v rozsahu ISMS a bude schválen odpovědným vedoucím. Organizace by měla přezkoumat přehled struktury v plánovaných intervalech, nebo pokud dojde k významným změnám (viz poznámka v AMC1 IS.I.OR.200(a)(1));

(b) identifikovat a kategorizovat všechny relevantní smluvní organizace používané k implementaci ISMS. Organizace by měla definovat a zdokumentovat postupy pro správu rozhraní a koordinaci mezi touto organozací a jinými organizacemi, včetně smluvních organizací;

(c) identifikovat a definovat všechny klíčové procesy a postupy a systémy interních a externích hlášení, které budou použity k udržení souladu s cíli tohoto nařízení po dobu životního cyklu ISMS. Organizace může upravit stávající procesy nebo postupy pro vyhovění;

(d) identifikovat a zdokumentovat jakékoli další informace, které budou použity k udržení shody s cíli tohoto nařízení;

(e) při vytváření a aktualizaci dokumentovaných informací zajistit vhodnou identifikaci a popis (např. název, datum, autor nebo referenční číslo), jakož i přezkoumání a schválení vhodnosti a přiměřenosti;

(f) kontrolovat dokumentované informace požadované ISMS, aby bylo zajištěno, že jsou:

(1) dostupné a vhodné pro použití tam, kde a kdy jsou potřeba;

(2) adekvátně chráněny (např. proti ztrátěu důvěrnosti, nesprávnému použití nebo ztrátě integrity).

GM1 IS.I.OR.200(c) Systém řízení bezpečnosti informací (ISMS)

Množství informací, které by měly být zdokumentovány, aby byla zachována shoda s cíli tohoto nařízení, se může mezi organizacemi lišit v důsledku různých faktorů, jako je velikost a složitost nebo potřeba harmonizace s jinými již zavedenými procesy řízení. Jako obecné vodítko, s přihlédnutím k dokumentům požadovaným pro vyhovění bodu IS.I.OR.200(a), požadavkům na vedení záznamů uvedeným v IS.I.OR.245 a požadavků na příručku pro řízení bezpečnosti informací uvedených v IS.I.OR.250, je níže uveden neúplný výčet informací, které by měly být zdokumentovány:

(a) politika informační bezpečnosti informací, která by měla zahrnovat cíle organizace v oblasti bezpečnosti informací – viz IS.I.OR.200(a)(1);

(b) zodpovědnosti *(responsibility* – kdo je odpovědný za vykonání svěřeného úkolu*)* a odpovědnosti *(accountablity* – kdo je odpovědný za celý úkol, je odpovědný za to, co je vykonáno*)* pro role související s bezpečností informací – viz IS.I.OR.250(a)(2), (3), (6) a (7) a požadavky na personál uvedené v bodech IS.I.OR.240(a), (b), (c), (d) a (f) a související AMC a GM;

(c) rozsah ISMS a rozhraní s jinými stranami a závislosti na nich – viz IS.I.OR.200(a)(2) a požadavky na bezpečnost informací uvedené v bodech IS.I.OR.205 (a) a (b);

(d) proces řízení rizik v oblasti bezpečnosti informací – viz požadavky na bezpečnost informací uvedené v bodech IS.I.OR.205 a IS.I.OR.210;

(e) archiv rizik identifikovaných v posouzení rizik v oblasti bezpečnosti informací spolu se souvisejícími opatřeními pro řešení rizik (často označovaný jako „registr rizik“ nebo „kniha rizik“) – viz IS.I.OR.245;

(f) důkaz o způsobilosti (kompetencích) nezbytné pro personál vykonávající činnosti požadované tímto nařízením – viz IS.I.OR.240(g) a související AMC a GM;

(g) důkaz o aktuálnosti způsobilosti (kompetencích) personálu vykonávajícího činnosti požadované tímto nařízením – viz IS.I.OR.245(b)(1);

(h) (klíčové) ukazatele výkonnosti odvozené z důkazů o monitorování a měření procesů ISMS.

GM1 IS.I.OR.200(d) Systém řízení bezpečnosti informací (ISMS)

PROPORCIONALITA PŘI IMPLEMENTACI ISMS

Při zavádění procesů a postupů a také při stanovování rolí a odpovědností požadovaných podle bodu IS.I.OR.200(d) by měla organizace především zvážit rizika, která může představovat pro jiné organizace, a také své vlastní vystavení riziku. Mezi další aspekty, které mohou být relevantní, patří potřeby a cíle organizace, požadavky na bezpečnost informací, jeho vlastní procesy a velikost, složitost a struktura organizace, které se mohou v průběhu času měnit.

IMPLEMENTACE ISMS S PODPOROU

V kontextu Části IS iniciují všechny organizace implementaci ISMS určením jeho rozsahu, který je zase založen alespoň na posouzení dopadů na bezpečnost letectví, pro které jsou incidenty týkající se bezpečnosti informací příčinou nebo přispívajícím faktorem. Organizace, bez ohledu na svou velikost, nemusí mít ještě dostatečné znalosti o svých rizicích informační bezpečnosti a mohou zvážit, zda vyhledají podporu u poskytovatele služeb, který může také poskytnout další personál a odborné znalosti během této implementační fáze ISMS. Totéž může platit pro pozdější fáze implementace ISMS a za tímto účelem mohou organizace chtít zvážit ustanovení IS.I.OR.235 a související AMC. Outsourcing specifických funkcí ISMS, jako je monitorování bezpečnosti informací nebo reakce na incidenty poskytovatelům služeb, může pomoci zajistit, aby organizace měla přístup ke zkušeným pracovníkům a odborným znalostem. Podobně mohou organizace chtít, aby je poskytovatel služeb podporoval při provádění posuzování rizik.

Pokud jde o ustanovení vhodného personálu pro zavádění a dodržování ustanovení tohoto nařízení, organizace by se měly vždy odvolávat na AMC1 IS.I.OR.240(f) a GM1 IS.I.OR.240(f) s tím, že více odpovědností může být přiděleno jedné osobě, přičemž je vždy zajištěna nezávislost sledování shody.

Jako úvod k povaze rizik bezpečnosti informací a jejich řízení mohou organizace jako prvotní vodítko použít meziagenturní zprávu NIST Interagency Report (NISTIR 7621 Rev. 1) *„Small Business Information Security: The Fundamentals“*.

ZAČLENĚNÍ ISMS PODLE TOHOTO NAŘÍZENÍ DO STÁVAJÍCÍCH SYSTÉMŮ ŘÍZENÍ

Organizace může při implementaci ISMS využít výhod stávajících systémů řízení tím, že jej integruje do těchto stávajících systémů.

Integrací ISMS do stávajících systémů řízení může organizace snížit úsilí a náklady potřebné k zavedení a udržování ISMS a zároveň zajistit konzistenci a soulad s celkovým přístupem organizace k řízení. Níže je uveden neúplný seznam potenciálních synergií, které lze využít při integraci ISMS do stávajícího systému řízení:

— Využít stávajících zásad a postupů: organizace může použít své stávající zásady a postupy jako základ pro svůj ISMS. To může pomoci zajistit konzistenci a minimalizovat potřebu další dokumentace.

— Sladit ISMS s jinými systémy řízení: organizace může sladit ISMS s jinými systémy řízení, jako jsou systémy řízení bezpečnosti (SMS), aby zajistil, že ISMS bude v souladu s celkovým přístupem organizace k řízení.

— Použít stávající procesy řízení rizik: organizace může použít své stávající procesy řízení rizik k identifikaci a posouzení rizik v oblasti bezpečnosti informací, která mohou vést k rizikům bezpečnosti letectví.

— Znovu použít existující kontroly/opatření: organizace může znovu použít stávající opatření, jako jsou kontroly přístupu nebo proces řízení incidentů, k implementaci opatření v oblasti bezpečnosti informací požadovaných ISMS.

— Proces neustálého zlepšování: organizace může využívat proces neustálého zlepšování stávajících systémů řízení ke zlepšení ISMS v průběhu času.

AMC1 IS.I.OR.200(e) Systém řízení bezpečnosti informací (ISMS)

VÝJIMKA

Aby požádaly o schválení výjimky příslušným úřadem podle bodu IS.I.OR.200(e), měly by se organizace řídit pokyny uvedenými v AMC1 IS.I.OR.205(a) a AMC1 IS.I.OR.205(b) k provedení zdokumentovaného posouzení rizik bezpečnosti informací. Aby se opodstatnily důvody pro výjimku, očekává se, že posouzení rizik poskytne vysvětlení pro vyloučení všech prvků z oblasti působnosti ISMS. Je na úřadu, aby určil, zda je toto posouzení pro udělení výjimky považováno za dostatečné.

Organizace, které by chtěly, aby posouzení rizik provedla třetí strana, by měly zvážit požadavky IS.I.OR.235 a související AMC.

GM1 IS.I.OR.200(e) Systém řízení bezpečnosti informací (ISMS)

Jakákoli organizace, která se domnívá, že nepředstavuje žádné riziko pro bezpečnost informací s potenciálním dopadem na bezpečnost letectví, ať už pro ni samotnou nebo pro jiné organizace, může zvážit, že u příslušného úřadu požádá o schválení výjimky podle postupu popsaného v AMC1 IS.I.OR.200(e).

Některé příklady organizací, které mohou zvažovat žádost o výjimku, mohou zahrnovat:

— Letecký provozovatel, který provádí obchodní jiný než vysoce rizikový zvláštní provoz (SPO) s nesložitými letadly, pokud povaha provozu opodstatňuje výjimku.

— Letecký provozovatel, který provozuje letadlo ELA2, jak je definováno v čl. 1 odst. 2 písm. j) nařízení (EU) č. 748/2012, s výjimkou jednoho letadla, které je provozováno za předem stanovených provozních podmínek nebo za určitých provozních omezení.

— Organizace oprávněná k údržbě podle Části 145, která se zabývá pouze údržbou letadlových celků nebo činnostmi údržby, které nepřispívají k zajištění strukturální integrity letadla ani žádných významných funkcí souvisejících s bezpečností – například provádění činností, jako je mytí, odstraňování nátěrů, lakování atd.

Výše uvedené příklady nejsou vyčerpávající a jsou pouze orientačními potenciálními scénáři, které by mohly poskytnout prvotní základ pro přípravu posouzení rizik bezpečnosti informací, které opodstatňuje vyloučení všech prvků organizace z působnosti ISMS.

GM1 IS.I.OR.205 Posouzení rizik bezpečnosti informací

Část IS nevyžaduje použití žádného specifického rámce zabezpečení informací, jako je ISO, NIST nebo jiné, k vypracování posouzení rizik nebo obecně k implementaci řízení rizik. Každý rámec nabízí různé výhody a žádný z těchto rámců není pro jednotlivou organiizaci dokonalý a měl by být přizpůsoben a upraven tak, aby splňoval celkové potřeby organizace, jakož i konkrétní potřebu zohlednit aspekty bezpečnosti letectví.

Organizace, jejíž rámce bezpečnosti informací získaly průmyslovou certifikaci, může tyto informace poskytnout jako podpůrné artefakty; tyto organizace by však měly prokázat použitelnost průmyslové certifikace na oblast působnosti tohoto nařízení (viz GM1 IS.I.OR.200).

Obecné pokyny pro řízení rizik, včetně posuzování rizik, lze nalézt v ISO/IEC 27005 a ISO/IEC 31000 a také v NIST SP 800-30. Organizace v letectví mohou také zvážit pokyny specifické pro letectví, jak jsou definovány v kapitole řízení rizik v nejnovější verzi EUROCAE ED-201A a podle vhodnosti pro konkrétní provozní prostředí v kapitolách EUROCAE ED-204A, EUROCAE ED-205A a EUROCAE ED-206 pokrývajících řízení rizik.

AMC1 IS.I.OR.205(a) Posouzení rizik bezpečnosti informací

Při provádění posouzení rizik v oblasti bezpečnosti informací by měla organizace zajistit, aby byly identifikovány všechny příslušné prvky bezpečnosti letectví a zahrnuty do rozsahu ISMS podle IS.I.OR.200 a souvisejících AMC.

Způsob, jak vyhovět požadavku v bodě IS.I.OR.205(a), je provést předběžné posouzení rizik na vysoké úrovni nebo posouzení dopadů, provedené v souladu s dokumentovanou metodikou a podle přesných kritérií pro zahrnutí a vyloučení z rozsahu ISMS prvků uvedených v IS.I.OR.205(a).

GM1 IS.I.OR.205(a) Posouzení rizik bezpečnosti informací

IDENTIFIKACE ROZSAHU A HRANIC

Organizace by měla jasně a komplexně porozumět svým činnostem a službám v oblasti letectví, souvisejícím procesům a s tím spojeným informačním systémům a příslušným datovým tokům a výměnám informací, které definují rozsah ISMS a hranice pro posouzení rizik. Organizace by proto měla vypracovat odpovídající dokumentaci o zdrojích a závislostech souvisejících s výpočetní technikou, sítí a smluvními službami, které mají potenciál ovlivnit informační bezpečnost a bezpečnost funkcí, služeb nebo schopností v rámci posouzení rizik.

Následující neúplný seznam uvádí příklady položek, které lze vzít v úvahu pro identifikaci výše uvedeného rozsahu a hranic. Úroveň podrobnosti analýzy může být iterativní proces, s úsilím úměrným očekávané úrovni rizika. Jak je uvedeno výše, účelem je získat znalosti o všech relevantních aktivech, zdrojích a závislostech, které jsou přímou součástí funkcí, služeb a schopností, prostřednictvím následujících činností:

(a) Identifikace provozních vstupů a výstupů relevantních pro funkce, služby a schopnosti organizace; mohou souviset s:

- interními nebo externími zdroji;
- interními nebo externími pronajímanými nebo spravovanými službami nebo jinými závislostmi;

(b) Identifikace všech příslušných aktiv (tj. hardwaru, softwaru, sítě a výpočetních zdrojů) používaných k vytváření, zpracování, přenosu, ukládání nebo přijímání výše uvedených provozních vstupů a výstupů;

(c) Identifikace provozních prostředí (např. kancelář, veřejný prostor, místnost s kontrolovaným přístupem atd.) a umístění všech relevantních aktiv;

(d) U každého aktiva zahrnutého v rozsahu identifikace konkrétních metod, procesů a zdrojů, které budou použity ke správě, provozu a údržbě každého aktiva během jeho životního cyklu, včetně:

- interních nebo smluvních zdrojů;
- smluvních společností vzdáleně spravujících aktiva (tj. poskytovatele spravovaných služeb).

AMC1 IS.I.OR.205(b) Posouzení rizik bezpečnosti informací

Organizace by měla v rámci posouzení rizik bezpečnosti informací určit rozhraní, která má s jinými stranami, jako jsou poskytovatelé služeb, dodavatelské řetězce a další třetí strany, na základě výměny dat a informací a aktiv používaných pro tuto výměnu, což by mohlo vést k situaci, kdy rizika informační bezpečnosti v důsledku vzájemného vystavení mohou buď:

- zvýšit rizika pro bezpečnost letectví, kterým čelí ostatní strany; a/nebo
- zvýšit rizika pro bezpečnost letectví, kterým čelí organizace.

GM1 IS.I.OR.205(b) Posouzení rizik bezpečnosti informací

SDÍLENÍ INFORMACÍ O RIZICÍCH

Organizace tvořící rozhraní by si měly navzájem sdílet informace o možném vystavení rizikům informační bezpečnosti, například podle postupu popsaného v EUROCAE ED-201A, Appendix B – B.1, B.2 a B.3. Účelem této výměny informací je umožnit organizacím vytvořit odpovídající mapování pro služby uvedené v IS.I.OR.205(a), včetně všech informačních a datových toků, s cílem:

(a) ilustrovat (např. prostřednictvím funkčního diagramu) vztahy logických a fyzických cest spojujících různé zúčastněné strany;

(b) jasně identifikovat všechna aktiva (tj. hardware, software, síť a výpočetní zdroje), která budou při výměně použita;

(c) identifikovat všechny funkce, činnosti a procesy, včetně jejich příslušných informací a dat, které budou vytvářeny, přenášeny, zpracovávány, přijímány a ukládány, a spojit je s odpovědnou stranou, která tyto funkce, činnosti a procesy poskytuje nebo vykonává;

(d) určit pro tyto cesty, tvořící tzv. funkční řetězce, roli strany tvořící rozhraní, jako je výrobce, zpracovatel, odesílatel nebo spotřebitel příslušných informací nebo dat;

(e) určit, zda jedna strana tvořící rozhraní působí jako původce nebo příjemce toku přes takovou cestu.

DVĚ KATEGORIE ORGANIZACÍ Z POHLEDU ROZHRANÍ

Existují dvě kategorie organizací tvořících rozhraní: ty, na něž se vztahuje nařízení (EU) 2023/203 nebo nařízení (EU) 2022/1645, a ty, na něž se nevztahuje.

Pokud má daná organizace rozhraní s organizací, na niž se vztahuje nařízení (EU) 2023/203 nebo nařízení (EU) 2022/1645, každý subjekt:

— je odpovědný za identifikaci rozhraní, která má jeho vlastní organizace s jinými organizacemi a která by mohla mít za následek vzájemné vystavení se rizikům bezpečnosti informací. Subjekt může mít prospěch ze sdílení informací o rizicích, protože tato výměna umožňuje přesnější posouzení těchto rizik;

— zůstává odpovědný za řádné řízení rizik informační bezpečnosti v rámci svého vlastního ISMS.

Ve všech ostatních případech je organizace odpovědná za řádné řízení rizik bezpečnosti informací, která mohou vyplynout z jeho vystavení subjektu tvořícímu rozhraní. Tam, kde je třeba tato rizika řešit, má organizace vždy možnost zavést zmírňující opatření a kontroly v rámci svých vlastních hranic. Ve zvláštním případě, kdy je subjektem tvořícím rozhraní dodavatel, může organizace rozhodnout o řízení rizik prostřednictvím smluvních ujednání a požadovat, aby dodavatel zavedl zmírňující opatření a kontroly v rámci své vlastní organizace.

GM2 IS.I.OR.205(b) Posouzení rizik bezpečnosti informací

PŘÍKLADY LETECKÝCH SLUŽEB

Příklady leteckých služeb, které lze vzít v úvahu při určování rozsahu a rozhraní ISMS, jsou uvedeny v Dodatku III.

AMC1 IS.I.OR.205(c) Posouzení rizik bezpečnosti informací

Organizace by měla používat rámec řízení rizik, který zahrnuje metodiku pro přiřazování rizik k úrovni rizika a stanovení kritérií pro určení přijatelnosti rizik nebo dalšího řešení.

Organizace by měla poskytnout zdokumentované důkazy o posouzení rizik, která mají potenciální dopad na bezpečnost letectví, včetně úrovně rizik. Organizace by měla spojit každé riziko s příslušnými

prvky a rozhraními uvedenými v IS.I.OR.205 (a) a (b) a zdokumentovat, zda je riziko přijatelné nebo vyžaduje další řešení.

Organizace by měla poskytnout záruku, že proces posuzování rizik je prováděn s nezbytnou pečlivostí a kázní, a to dokumentací procesu a jeho robustnosti. Přitom by měla organizace zvážit:

(a) reprodukovatelnost a výsledků posouzení v případě podobných vstupů;

(b) opakovatelnost posouzení v čase takovým způsobem, že výsledky různých předchozích posouzení lze porovnat a určit změny;

(c) shromažďování vstupů, které jsou relevantní a platné, zejména:

(1) informace, které umožňují určit důsledky pro bezpečnost;

(2) informace, které umožňují určit potenciál výskytu scénáře hrozby;

(d) iterativní zdokonalování v průběhu času umožňující zpřístupnění detailnějších scénářů hrozeb jako vstupů s cílem snížit nejistotu ohledně hrozeb, zranitelnosti, účelnosti stávajících kontrol/opatření a závislostí na externích subjektech, a to zejména:

(1) zdokonalování počátečních scénářů hrozeb na vysoké úrovni s většími podrobnostmi a specifičností, jak se shromažďuje více dat;

(2) zpřesňování údajů o známých zranitelnostech průběžnou aktualizací informací o jejich zneužitelnosti a souvisejících důsledcích;

(3) přezkoumávání účelnosti stávajících kontrol/opatření a zvážení nově dostupných kontrol/opatření;

(4) upřesnění chápání závislostí na externích subjektech a jejich důsledků pro rizikový profil organizace.

GM1 IS.I.OR.205(c) Posouzení rizik bezpečnosti informací

POSOUZENÍ RIZIK

Mohou být použity níže uvedené úrovně klasifikace rizik pro potenciální výskyt scénáře hrozby a závažnost bezpečnostních důsledků; to však nebrání organizaci ve vytvoření dalších přechodných kategorií, pokud to považuje za nezbytné pro posouzení rizik. Organizace by měla specifikovat a zdokumentovat použité úrovně klasifikace specifické pro organizaci s přesnou kvalitativní nebo kvantitativní definicí, pokud jde o rozsah nebo interval číselných hodnot, aby umožnil dostatečně kalibrovaný, konzistentní odhad, hodnocení a komunikaci v rámci organizace nebo se subjekty tvořícími rozhraní. Potenciál výskytu scénáře hrozby lze vyjádřit jako interval pravděpodobností včetně doby trvání pozorování. Podpůrnou dokumentaci a metody lze nalézt v EUROCAE ED-203A, kapitola 3.6, která odkazuje na vyhodnocení potenciálu výskytu scénáře hrozby v posouzení bezpečnostních rizik EUROCAE ED-202A.

Poznámka 1: Výraz „trvání pozorování“ se vztahuje k časovému období, během kterého je scénář hrozby pozorován nebo monitorován. Je zásadní při určování pravděpodobnosti naplnění scénáře hrozby, protože pravděpodobnost výskytu se může lišit v závislosti na délce sledovaného období.

Poznámka 2: EUROCAE ED-202A a EUROCAE ED-203A byly původně vypracovány pro posuzování rizik bezpečnosti informací v letadlech, ale obecné principy vytvořené v těchto dokumentech mohou být přizpůsobeny jiným rámcům, pokud to organizace považuje za užitečné.

Aby se usnadnila vzájemná srovnatelnost metodik posuzování rizik mezi organizacemi tvořícími rozhraní, může organizace přiřadit posouzení potenciálu výskytu scénáře hrozby k jedné z následujících kategorií:

— Vysoký potenciál výskytu: scénář hrozby pravděpodobně nastane. Útok související se scénářem hrozby je proveditelný a podobné scénáře hrozby se v minulosti vyskytly mnohokrát.

— Střední potenciál výskytu: scénář hrozby pravděpodobně nenastane. Útok související se scénářem hrozby je možný a k podobnému scénáři hrozby mohlo v minulosti dojít.

— Nízký potenciál výskytu: scénář hrozby je velmi nepravděpodobný. Naplnění scénáře hrozby je teoreticky možné; není však známo, že k němu došlo.

Hodnocení potenciálu výskytu scénáře hrozby může být založeno na následujících aspektech:

Ochrana (jak je definováno v EUROCAE ED-203A)

— Bezpečnostní opatření a architektura, které odmítají přístup k aktivům: míra, do jaké je aktivum otevřené přístupu z kompromitovaných systémů

— Přístup k bezpečnostním opatřením: míra, do jaké bezpečnostní opatření brání přístupu/útoku na sebe z kompromitovaných systémů

— Selhání mechanismu: míra, do jaké známá implementace bezpečnostního opatření selže při zabránění útoku

— Detekční metody nebo postupy pro rozpoznání útoku a vhodnou reakci, aby se snížila možnost výskytu scénáře hrozby

Snížení expozice (jak je definováno v EUROCAE ED-203A)

— Podmínky, za kterých může uživatel nebo útočník použít externí přístupové připojení

— Omezení funkčnosti externího přístupového připojení

— Organizační zásady, které kontrolují dobu proveditelnosti pro vývoj nástrojů útoku specifických pro daný produkt

— Management (správa) zranitelností včetně zpravodajské činnosti, skenování, řešení a opakovaného testování zaměřených na odhalení, detekci a řešení hlášených nebo zjištěných zranitelností rychlým způsobem s ohledem na prioritu rizika při vysoké jistotě, aby se omezila plocha, kudy se dá provést útok

— Snížení závažnosti úspěšného útoku (tj. prostřednictvím redundantního systému, který může zachovat kontinuitu služby v případě odepření služby systému kritického pro bezpečnost letectví)

Pokus o útok (jak je definováno v EUROCAE ED-203A)

— Schopnost útočníků, která je určována zdroji a odbornými znalostmi potřebnými k jejich útoku

Schopnost útočníků lze posoudit prostřednictvím několika způsobů, například:

— informací týmů CERT *(computer emergency response teams)* / CSIRT *(computer security incident response teams)*, středisek pro sdílení a analýzu informací (ISAC);

— analýz minulých aktivit, taktik, technik a postupů (TTP) a úspěšnosti útoků.

Ze stejného důvodu může organizace přiřadit výsledek hodnocení závažnosti bezpečnostních důsledků k jedné z následujících kategorií:

— Vysoká závažnost: ty scénáře, které mohou okamžitě nebo se zpožděním způsobit nebo přispět k nebezpečnému stavu, kdy nebezpečný stav znamená událost spojenou s provozem letadla, při které:

  — je osoba smrtelně nebo vážně zraněna;

  — letadlo utrpělo poškození nebo konstrukčnímu selhání;

  — letadlo je buď nezvěstné, nebo je zcela nedostupné;

— Střední závažnost: ty scénáře, které mohou okamžitě nebo se zpožděním způsobit bezpečnostní incidenty nebo k nim přispět, kdy incident znamená jakoukoli jinou událost než nehodu spojenou s provozem letadla, která ovlivňuje nebo by mohla ovlivnit bezpečnost provozu;

— Nízká závažnost: ty scénáře, které mohou okamžitě nebo se zpožděním způsobit nebo přispět k zanedbatelným bezpečnostním následkům.

Příklady vysoké, střední a nízké závažnosti lze pro produkty, systémy ATM a vzdušný prostor nalézt v EUROCAE ED-201A, Appendix B.

Pokud organizace nemůže určit vliv na bezpečnost, posouzení by mělo určit předpoklady z informací o sdílení rizik na rozhraních s jinými organizacemi ve funkčním řetězci, což vede k vlivu na bezpečnost.

Některé z těchto předpokladů lze zajistit certifikací produktů: tam, kde aktiva podléhají certifikaci produktu podle jiných leteckých předpisů týkajících se bezpečnosti informací o produktu, může organizace provádějící posouzení rizik považovat perimetr certifikace produktu za již pokrytý. To by mělo být přijatelné za podmínky, že tato certifikace je platná a že organizace implementovala pokyny poskytnuté výrobcem OEM pro zachování platnosti certifikace.

Další informace lze nalézt také v nařízení (EU) 2015/1018 o povinném hlášení událostí. Další příklady klasifikace závažnosti dopadů pro oblasti letectví lze nalézt v EUROCAE ED-201A, Appendix B – tabulky B-5, B-6 a B-7.

Kritéria přijatelnosti rizik

Kritéria přijatelnosti rizik jsou kritická a měla by být vyvíjena, specifikována a zdokumentována. Kritéria mohou definovat více prahových hodnot s požadovanou cílovou úrovní rizika, ale umožňují také odpovědnému vedoucímu nebo delegované osobě (delegovaným osobám) přijmout rizika nad touto úrovní za definovaných okolností a podmínek.

Aby se usnadnila vzájemná srovnatelnost posuzování rizik mezi subjekty tvořícími rozhraní, měla by organizace klasifikovat rizika do následujících kategorií:

— riziko nepřijatelné;

— riziko podmínečně přijatelné;

— riziko přijatelné.

Pokud jde o podmínečnou přijatelnost rizik, kritéria pro přijatelnost by měla brát v úvahu, jak dlouho se očekává, že riziko bude existovat (dočasná nebo krátkodobá aktivita nebo expozice), nebo mohou zahrnovat požadavky na závazek budoucích řešení ke snížení rizika na přijatelnou úroveň v rámci definované doby trvání a ukazují, jak bude riziko řízeno v průběhu času prostřednictvím procesů řízení rizik organizace.

Rizika by navíc měla být podmínečně přijata pouze za podmínky, že organizace prokáže existenci komplexní struktury řízení rizik, která zahrnuje procesy posuzování rizik, řešení rizik a monitorování rizik pro provozy/operace. Řízení rizik by mělo vzít v úvahu variabilitu a konzistenci pravděpodobnosti hrozby, zranitelnosti, stávající kontroly/opatření, externí závislosti a dopad na bezpečnost. Toho se obvykle dosáhne, když organizace dosáhne vyšší úrovně vyspělosti, která je reprezentativní pro funkčnost a opakovatelnost řízení rizik v oblasti bezpečnosti informací – viz GM1 IS.I.OR.260(a).

Následující Obrázek 1 znázorňuje matici přijatelnosti rizik založenou na výše uvedených kategoriích, kterou mohou používat organizace tvořící rozhraní pro vzájemnou srovnatelnost.

ICAO Annex 13 >	Zanedbatelný vliv	Incident	Nehoda
Potenciál výskytu scénáře hrozby	**Nízké bezpečnostní důsledky**	**Mírné bezpečnostní důsledky**	**Vysoké bezpečnostní důsledky**
Vysoký	Podmínečně přijatelné	Nepřijatelné	Nepřijatelné
Střední	Přijatelné	Podmínečně přijatelné	Nepřijatelné
Nízký	Přijatelné	Přijatelné	Podmínečně přijatelné*

Obrázek 1: Příklad matice přijatelnosti rizik pro srovnávací účely

* Potenciál výskytu scénáře hrozby je včas přehodnocen (viz IS.I.OR.205(d)) a monitorován, aby bylo zajištěno, že zůstane nízký a že pokud se riziko naplní, bude včas odhaleno a řešeno.

Komplexní struktura řízení rizik obvykle zahrnuje následující aspekty a procesy:

— opakovatelné a reprodukovatelné posouzení rizik. Jsou-li rizikové faktory považovány za značně nejisté a v nějakém širokém rozmezí hodnot nebo nejsou-li dostatečně přesné, provedou se další iterace posouzení rizik zahrnující dodatečně shromážděné nebo podrobné informace a podrobnější posouzení, aby se snížila nejistota a zvýšila přesnost;

— důkladný přezkum těchto rizik navržených jako podmíněně přijatelná, který provede odpovědný vedoucí nebo delegovaná osoba (osoby), která (který) může uložit další podmínky pro zachování rizik, včetně opatření pro řešení rizik a časového harmonogramu jeho provedení;

— striktní monitorování klíčových ukazatelů rizik, které zahrnuje definovanou a spolehlivou detekci možného vývoje materializace rizik;

— je zaveden systém reakce na incidenty s reaktivními opatřeními, která jsou spouštěna detekčními mechanismy, aby se okamžitě zamezilo důsledkům, zejména u rizikových scénářů s vysokou úrovní závažnosti.

Poznámka: Jak je podrobně popsáno v NIST SP-800 Rev.1, opakovatelnost se týká schopnosti opakovat posouzení v budoucnu způsobem, který je konzistentní a tedy srovnatelný s předchozími posouzeními – což organizaci umožňuje identifikovat trendy. Proto lze proces posouzení rizik klasifikovat jako „opakovatelný“, pokud za podobných podmínek subjekt nebo osoba poskytuje konzistentní výsledky.

Jak je podrobně popsáno v NIST SP-800 Rev.1, reprodukovatelnost se týká schopnosti různých odborníků produkovat stejné výsledky ze stejných dat. Proces posouzení rizik lze proto klasifikovat jako „reprodukovatelný“, když jiný subjekt nebo osoba může při stejných vstupech, předpokladech, kontextu bezpečnosti informací a prostředí hrozeb replikovat stejné kroky a dospět ke stejným závěrům.

Identifikace scénáře hrozby

Scénář hrozby je jedním z možných způsobů, jak by se hrozba mohla zhmotnit. Scénář hrozby obvykle popisuje potenciální útok zaměřený na jednu nebo více zranitelných míst aktiv, stejně jako procesů.

Účelem identifikace scénáře hrozby podle tohoto nařízení je vypracovat seznam scénářů, které mohou vést k ohrožení bezpečnosti informací s dopadem na bezpečnost letectví.

Scénář hrozby je obecně charakterizován následujícím:

— zdroj hrozby útoku na bezpečnost informací;

— vektor útoku a cesta přes organizaci až k aktivu;

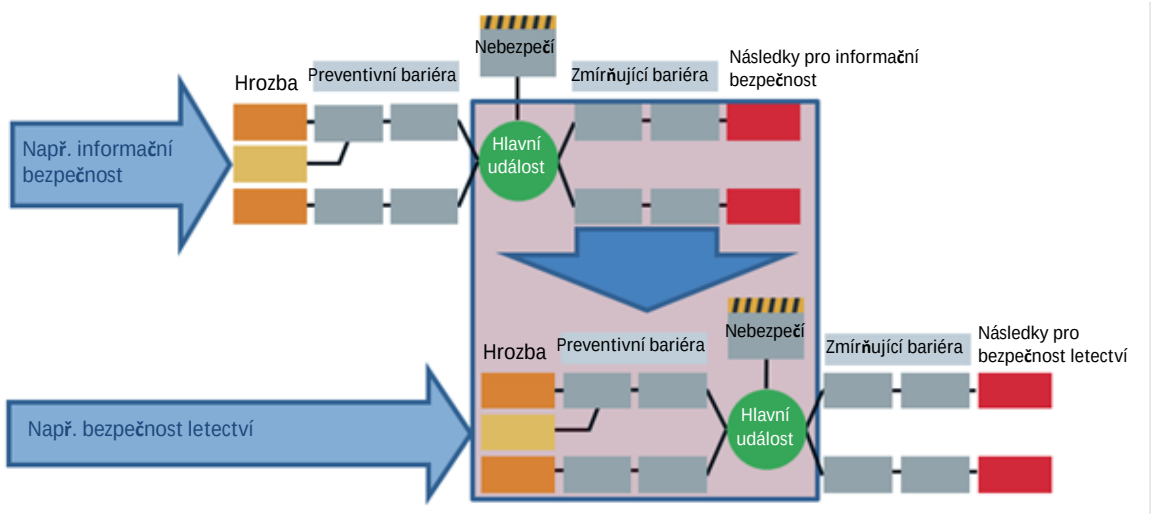
— kontroly/opatření bezpečnosti informací, které by zmírnily útok;

— důsledek útoku včetně dotčených bezpečnostních aspektů.

Pokyny pro identifikaci scénáře hrozeb lze nalézt v EUROCAE ED-202A, kapitola 3.4. Toto není jediný zdroj, kde lze nalézt pokyny, a organizace se může odvolávat na jiné pokyny, které jsou pro jejich použití vhodnější.

Další metody k identifikaci relevantních scénářů hrozeb

Při provádění této analýzy by měly být v průběhu procesu koordinovány aspekty bezpečnosti informací a bezpečnosti, aby bylo zajištěno vzájemné porozumění aplikovaným preventivním opatřením a opatřením ke zmírnění hrozeb. Na následujícím 0brázku 2 jsou interakce mezi bezpečností informací a bezpečností letectví znázorněny prostřednictvím „motýlkového“ diagramu, který zdůrazňuje vazby mezi kontrolami rizik a základním systémem řízení.



Obrázek 2: Interakce mezi oblastmi řízení rizik bezpečností informací a bezpečnosti letectví

Poznámka: Preventivní bariéra nebo opatření je proaktivní akce nebo kontrola implementovaná za účelem snížení pravděpodobnosti naplnění rizika, nebezpečí nebo hrozby, zatímco zmírňující opatření je akce nebo kontrola navržená ke snížení závažnosti nebo dopadu nežádoucí události, pokud by k ní došlo.

Příklady scénářů hrozeb

Katalogy hrozeb mohou poskytnout návod a prvky pro vypracování scénářů hrozeb, které jsou pro organizaci relevantní. Odkazy lze nalézt v ARINC 811 – Att. 3 – Tabulky 3-7 a 3-8 pro příklady katalogů hrozeb a další příklady katalogu hrozeb, jak je poskytují instituce EU – například taxonomie hrozeb ENISA. Toto však není vyčerpávající seznam příkladů, a proto by se identifikace scénářů hrozeb neměla omezovat pouze na tyto příklady. Kromě toho by měly být konzultovány další relevantní zdroje obsahující informace o hrozbách pro bezpečnost informací a o prostředí hrozeb pro bezpečnost informací, aby se příslušnými vstupy podpořil proces posuzování rizik.

Soubor příkladů scénářů hrozeb lze nalézt v Dodatku I.

AMC1 IS.I.OR.205(d) Posouzení rizik bezpečnosti informací

Organizace by měla při zjišťování souladu s cíli uvedenými v bodě IS.I.OR.205(d) vzít v úvahu následující kritéria:

(a) Posouzení rizik provedené podle bodů IS.I.OR.205 (a), (b) a (c) by mělo být v pravidelných intervalech přezkoumáváno, aby se identifikovaly a zohlednily příslušné změny. Periodicitu, s jakou musí být potenciální změny vyhodnoceny, by měla určit organizace provádějící posouzení s ohledem na kritičnost aktiv v rámci posouzení rizik, úrovně zbytkového rizika aktiv v rámci posouzení rizik a jakékoli smluvní nebo regulační požadavky. Vyšší kritičnost nebo úroveň rizika bude vyžadovat častější přezkoumání.

(b) Periodicita přezkumů posouzení rizik by měla být organizací zdokumentována a měla by zahrnovat zdůvodnění, datum schválení a informace o vlastníkovi rizika.

GM1 IS.I.OR.205(d) Posouzení rizik bezpečnosti informací

Kritéria, která je třeba zvážit pro četnost přezkumu posouzení rizik, může být úroveň rizika a také kritičnost a složitost příslušných aktiv. Cílem revize posouzení rizik je spustit přehodnocení rizik, jejich pravděpodobnosti a dopadu v případě relevantních změn. Jedním z možných způsobů je mít víceúrovňový přístup k posouzení rizik, přičemž pro identifikaci změn se používá posouzení rizik na vyšší úrovni. Posouzení rizik na vyšší úrovni by mohlo umožnit identifikaci podrobných rizik, která by

měla být přezkoumána v dalším kroku. Posouzení rizik by měla podléhat pravidelným přezkumům s cílem:

(a) umožnit neustálé zlepšování kvality posouzení rizik;

(b) zajistit efektivnost a účelnost kontrol rizik a zmírňujících opatření jak prostřednictvím jejich návrhu i provozu;

(c) přezkoumat plány a činnosti pro řešení rizik;

(d) identifikovat jakoukoli organizační změnu, která může vyžadovat přezkoumání priorit i řešení rizik;

(e) udržovat přehled o kompletním obrazu rizik; a

(f) identifikovat všechna vznikající rizika.

Přezkoumání posouzení rizik by mělo zahrnovat vlastníky rizik, projektové týmy a případně další zúčastněné strany. Důkaz o přezkoumání posouzení rizik by měl být zdokumentován a měl by zahrnovat:

— doklad o schválení přezkumu určeným vlastníkem rizika; a

— zdůvodnění nebo podklad pro schválení přezkoumání vlastníkem rizika.

Takový důkaz může zahrnovat, ale neomezuje se na:

— zprávy, které představují formu dokumentace pro sledování rizik bezpečnosti informací, která mohou mít dopad na organizaci;

— dokumentaci posouzení rizik bezpečnosti informací;

— výpisy z registru obchodních nebo bezpečnostních rizik.

Periodicita přezkumů posouzení rizik by měla být organizací rovněž dokumentována v příručkách, procesech nebo postupech týkjících se bezpečnosti informací a měla by být v souladu s širšími činnostmi řízení změn a přezkumy řízení bezpečnosti informací. Další pokyny ke kritériím a četnosti přezkumu posouzení rizik lze nalézt v EUROCAE ED-201A, Chapter 4, a také v EUROCAE ED-205A, Chapter 3.2 (pro ATMS/ANS).

GM2 IS.I.OR.205(d) Posouzení rizik bezpečnosti informací

Níže jsou uvedeny příklady změn, které by měly být identifikovány během přezkumu posouzení rizik, protože mohou vyvolat aktualizaci posouzení rizik:

(a) došlo ke změně prvků podléhajících rizikům bezpečnosti informací, jak je uvedeno v IS.I.OR.205(a); změna prvků bude zahrnovat:

— doplnění nebo vyjmutí z rozsahu posouzení rizik jednotlivých prvků;

— změny návrhu nebo konfigurace prvků v rámci rozsahu posouzení rizik, které mají potenciál změnit výsledky posouzení rizik; nebo

— změny hodnot prvků v rozsahu posouzení rizik, které by potenciálně vyvolaly změny úrovní dopadů;

(b) došlo ke změně v rozhraních mezi danou organizací a dalšími organizacemi, s nimiž daná organizace sdílí rizika pro bezpečnost informací nebo na které se spoléhá při zmírňování rizik informační bezpečnosti (např. dodavatelské řetězce, poskytovatelé služeb, poskytovatelé cloudu a zákazníci), jak je uvedeno v IS.I.OR. 205(b), nebo mezi systémem v rozsahu posouzení rizik a jakýmikoli jinými propojenými systémy nebo v rizicích oznámených dané organizaci jinými organizacemi, jak je uvedeno v IS.I.OR.205(b), nebo vlastníky nebo manažery dalších systémů včetně:

— vytvoření nových rozhraní;

— odstranění stávajících rozhraní;

— změny stávajících rozhraní, které by mohly změnit výsledky posouzení rizik.

Poznámka: Některá organizační nebo systémová propojení mohou být s organizacemi, které nespadají do oblasti působnosti tohoto nařízení, jak je definováno v článku 2, a proto nepodléhají požadavkům Části IS. V takovém případě by tyto organizace měly být informovány o své odpovědnosti hlásit výše uvedené změny prostřednictvím smluvních ujednání a požadavků na hlášení mezi dotčenými organizacemi případ od případu a kde je to použitelné;

(c) došlo ke změně informací nebo znalostí používaných pro identifikaci, analýzu a klasifikaci rizik, včetně:

— změn hrozeb a jejich hodnot nebo přidání nových hrozeb, které dříve nebyly posouzeny;

— změn zranitelností nebo přidání nových zranitelností, které nebyly dříve posouzeny;

— změn dopadů nebo následků posuzovaných hrozeb nebo zranitelností;

— změn v agregaci rizik, které mohou vést k nepřijatelným úrovním rizik;

— změn nebo zlepšení v procesu řízení rizik, přístupu k posuzování rizik a souvisejících činnostech;

— změn nebo zlepšení v řešení rizik;

— změn v kritériích používaných k určení přijatelnosti a řešení rizik;

(d) existují ponaučení z analýzy incidentů v oblasti bezpečnosti informací, včetně:

— pochopení, proč a jak k incidentům došlo; a

— přezkoumání všech typů incidentů, včetně incidentů způsobených vnějšími faktory, technickými důvody nebo lidskými chybami (neúmyslné chování). U lidských úmyslných činů lze rozlišovat mezi maligními a benigními činy.

AMC1 IS.I.OR.205(e) Posouzení rizik bezpečnosti informací

POSOUZENÍ PODPORY BEZPEČNOSTI (SAFETY)

Poskytovatelé jiných služeb než ATS by měli provést posouzení podpory bezpečnosti, jak je popsáno v nařízení (EU) 2017/373, aby posoudili riziko bezpečnosti informací u svých aktiv s ohledem na specifikaci služby, např. integritu a dostupnost, a identifikovat zbytkové riziko.

Poskytovatel jiných služeb než ATS by měl vhodnou formou sdílet s poskytovatelem ATS informace o zbytkovém riziku a dopadu na služby, které tomuto poskytovateli ATS poskytuje.

Zbytkové riziko by se mělo použít k posouzení potenciálního dopadu na služby a produkty, které poskytovatel jiných služeb než ATS nabízí poskytovateli ATS.

Poskytovatel ATS může toto použít jako vstup pro své posouzení bezpečnostních (security) rizik a, což je důležitější, pro vyhodnocení potenciálních dopadů těchto zbytkových rizik na bezpečnost (safety).

GM1 IS.I.OR.205(e) Posouzení rizik bezpečnosti informací

POSOUZENÍ PODPORY BEZPEČNOSTI

Tabulka 1 níže uvádí poskytovatele jiných služeb než ATS, kteří musí splňovat Hlavu C Přílohy III nařízení (EU) 2017/373. Jedná se o organizace, které musí provádět posouzení podpory bezpečnosti, aby mohly poskytovat požadované informace poskytovatelům ATS.

Informace o dopadu na produkty a služby by mohly být sdíleny mezi poskytovateli jiných služeb než ATS a poskytovateli ATS prostřednictvím dohodnutých prostředků, např. dohody o úrovni služeb, externí dohody (v souladu s EUROCAE ED-201A) atd.

Sdílené informace by měly umožnit poskytovatelům ATS provést přesné posouzení zbytkového rizika pro jejich služby. Pokud například poskytovatelé jiných služeb než ATS identifikovali riziko, které by mohlo ovlivnit dostupnost dat poskytovaných poskytovateli ATS, měl by být dopad na dostupnost popsán způsobem, který tomuto poskytovateli ATS umožní posoudit, zda by výsledná latence nebo zpoždění datových přenosů mohly mít dopad na bezpečnost. To je důležité, protože pouze poskytovatel ATS prostřednictvím svého posouzení může zbytkové riziko buď přijmout, nebo odmítnout.

Tabulka 1: Poskytovatelé jiných služeb než ATS, kteří musí splňovat Hlavu C Přílohy III nařízení (EU) 2017/373

	Příloha III (Část ATM/ANS.OR)				Příloha IV (Část ATS)	Příloha V (Část MET)	Příloha VI (Část AIS)	Příloha VII (Část DAT)	Příloha VIII (Část CNS)	Příloha IX (Část ATFM)	Příloha X (Část ASM)	Příloha XI (Část FPD)	Příloha XII (Část NM)
	Hlava A	Hlava B	Hlava C	Hlava D									
Poskytovatelé letových provozních služeb	x	x		x	x								
Poskytovatelé meteorologických služeb	x	x	x	x		x							
Poskytovatelé leteckých informačních služeb	x	x	x	x			x						
Poskytovatelé datových služeb	x	x	x					x					
Poskytovatelé komunikačních, navigačních nebo přehledových služeb	x	x	x	x					x				
Poskytovatelé uspořádání toku letového provozu	x	x	x	x						x			
Poskytovatelé uspořádání vzdušného prostoru	x	x	x								x		
Poskytovatelé služeb tvorby letových postupů	x	x	x									x	
Manažer struktury vzdušného prostoru	x	x	x	x									x

GM1 IS.I.OR.210 Řešení rizik bezpečnosti informací

Nepřijatelná rizika identifikovaná v souladu s bodem IS.I.OR.205 vyžadují proces řešení rizik, který může vést k zavedení opatření pro bezpečnost informací, často označovaných jako kontroly bezpečnosti informací.

Pro každé identifikované riziko by organizace měla definovat konkrétní opatření, metody nebo zdroje pro řešení rizika, které budou během životního cyklu každého aktiva použity k:

— řízení snižování rizik;

— monitorování a udržování každého aktiva;

— aktualizaci a plnění činností pro správu konfigurace;

— řízení dodavatelského řetězce;

— řízení smluvních služeb nebo poskytovatele služeb.

Přezkoumání opatření k řešení rizik by mělo zahrnovat úvahy o životním cyklu, které zavádí zařízení, postupy a personál.

Plán řešení rizik jako výsledek procesu řízení rizik by měl zahrnovat stanovení priority rizik, odpovídající informace o cílech a způsobech řešení rizik, aby bylo dosaženo přijatelné úrovně rizika, a také dohodnuté časové harmonogramy specifikující, do kdy by měli odpovědní pracovníci mít provedena opatření k řešení rizik. Časové harmonogramy implementace opatření pro řešení rizik by měl odsouhlasit personál zodpovědný za implementaci a měl by být komunikován s odpovědným vedoucím nebo delegovanou osobou (osobami) a jím/jí/jimi akceptován.

Jakékoli následné zpoždění implementace, spolu s jeho příčinou, důvodem, odůvodněním nebo nutností, by mělo být zdokumentováno v plánu řešení rizik pro rizika, která mohou vést k nebezpečnému stavu. Aktualizované řešení rizika by mělo být sděleno příslušnému úřadu v případě, že by materializace rizika vedla k nebezpečnému stavu. Zpoždění je také podmíněno akceptací odpovědným vedoucím nebo delegovanou osobou (osobami). Tato osoba může takovou akceptaci podmínit zavedením nebo dostupností kompenzačních kontrol nebo reaktivních opatření ke sledování, včasné detekci a včasné reakci na materializaci rizika v řešení. Aby bylo možné reagovat včas, může být tým reakce na incident informován, aby zahájil svou připravenost.

Plán řešení rizik může sloužit jako prostředek komunikace s příslušným úřadem k prokázání účinného řešení nepřijatelných rizik. Podobně lze tento plán použít ke komunikaci mezi organizacemi tvořícími rozhraní, jak jsou řízena sdílená rizika.

V souladu s IS.I.OR.205(d) je nezbytný pravidelný nebo podmíněný přezkum posouzení rizik, což zahrnuje přezkum opatření k řešení rizik vypracovaných podle IS.I.OR.210(a) s cílem zjistit, zda jsou stále efektivní nebo vyžadují úpravy.

Kromě toho by organizace měla také zvážit potenciální dopad na účelnost opatření pro řešení rizik tam, kde může vzniknout riziko bezpečnosti sdílených informací v důsledku interakce mezi subjekty tvořícími rozhraní (viz IS.I.OR.235 a související AMC).

AMC1 IS.I.OR.210(a) Řešení rizik bezpečnosti informací

(a) Proces řešení rizik by měl dosáhnout alespoň jednoho z cílů uvedených v IS.I.OR.210(a).

(b) Při zjišťování souladu s cíli podle bodů IS.I.OR.210(a)(1) a IS.I.OR.210(a)(2) by měla organizace vzít v úvahu, že:

(1) opatření vypracovaná podle těchto bodů by měla být prováděna v souladu s plánem řešení rizik s definovanými prioritami založenými na riziku, cíli a dohodnutými časovými harmonogramy a vlastníky.

(2) hlediska životního cyklu by měla být identifikována a asociována, aby byla zajištěna nepřetržitá účelnost opatření pro bezpečnost informací, včetně výměny dat s jinými subjekty;

(3) měla by přezkoumat a aktualizovat posouzení rizik podle IS.I.OR.205(d) s cílem vyhodnotit, zda opatření vyvinutá podle těchto bodů zavádějí nová nepřijatelná rizika nebo pozměňují stávající rizika tak, že se stávají nepřijatelnými.

(c) Řešení rizik by mělo být zdokumentováno a zaznamenáno například v registru rizik, i když bylo riziku zabráněno.

AMC1 IS.I.OR.215(a)&(b) Systém interního hlášení v oblasti bezpečnosti informací

Organizace by měly využívat jako zdroj incidenty zjištěné během činností prováděných k prokázání vyhovění IS.I.OR.220(a). Organizace by měly mít mechanismus pro shromažďování oznámení o událostech od personálu a zdrojů mimo společnost, včetně dodavatelů, partnerů, zákazníků, softwaru s otevřeným zdrojovým kódem a výzkumníků v oblasti bezpečnosti informací. Mechanismus pro shromažďování informací personálem a externími zdroji by měl být snadno dostupný a sdělitelný.

Organizace by měla shromažďovat všechny události shromážděné prostřednictvím detekčních prostředků pro interní analýzu. Každá událost by měla být analyzována, aby se zjistilo, zda je možné ji hlásit, a pokud ano, jaký potenciální nebo skutečný dopad na bezpečnost letectví nastal. Události bezpečnosti informací by měly být zvažovány v kombinaci s jinými událostmi, aby byla zajištěna korelace k identifikaci incidentů nebo zranitelností s potenciálním dopadem na bezpečnost letectví.

Organizace by měla zvážit výsledek posouzení rizik a využitelnost nových zranitelných míst objevených během detekčních činností prováděných podle opatření požadovaných v IS.I.OR.220(a).

Organizace by měla identifikovat všechny interní zainteresované strany, které vyžadují oznámení o konkrétním incidentu nebo zranitelnosti, a zajistit, aby tyto zainteresované strany obdržely všechny nezbytné informace o incidentu nebo zranitelnosti, aby mohly účinně a včas jednat a podpořit požadované lhůty pro detekování a reakci.

GM1 IS.I.OR.215(a)&(b) Systém interního hlášení v oblasti bezpečnosti informací

VZTAH MEZI INTERNÍM A EXTERNÍM HLÁŠENÍM

Organizace by měly shromažďovat a hlásit interně incidenty a zranitelnosti s cílem pokrýt všechny položky v oblasti působnosti tohoto nařízení. Jak interní, tak externí hlášení jsou nezbytná pro kompletní a efektivní systém hlášení. Interní hlášení by měla být včas posouzenaa tam, kde je potenciální dopad na bezpečnost nebezpečným stavem, by organizace měly iniciovat hlášení těchto interních zpráv podle IS.I.OR.230.

GM2 IS.I.OR.215(a)&(b) Systém interního hlášení v oblasti bezpečnosti informací

ORGANIZACE SBĚRU A HODNOCENÍ UDÁLOSTÍ BEZPEČNOSTI INFORMACÍ

Ve velkých organizacích je běžnou praxí centralizovat operace týkajících se informační bezpečnosti v bezpečnostním operačním centru – SOC *(security operations centre)* a využívat systém správy událostí a informací v oblasti bezpečnosti informací – SIEM *(information security information and event management)*. Systém SIEM shromažďuje všechny události ze zdrojů, jako jsou protokolové soubory log, ve společné databázi a umožňuje analytikům a respondentům ve společném SOC tyto události kontrolovat a jednat podle nich. Organizace se mohou rozhodnout použít SOC pro události související s Částí IS samostatně nebo v kombinaci s událostmi, které nepodléhají Části IS, ale které jsou pro organizaci zajímavé, jako jsou události související s obchodními zájmy. Události lze automaticky agregovat, korelovat a analyzovat, aby bylo možné odhalit abnormální chování vedoucí k incidentům bezpečnosti informací.

Organizace, které nemají schopnost SOC a nepoužívají systém SIEM, musí zvážit, jak zavést procesy, aby splnily požadované schopnosti sběru a vyhodnocování a také lhůty pro detekování a reakce.

GM3 IS.I.OR. 215(a)&(b) Systém interního hlášení v oblasti bezpečnosti informací

RELEVANTNÍ INFORMACE TÝKAJÍCÍ SE INCIDENTŮ A ZRANITELNOSTÍ

Pochopení příčin a faktorů přispívajících k incidentům a zranitelnostem bezpečnosti informací v souvislosti s Částí IS umožňuje získat poučení a vnést nápravu do procesů a návrhu aktiv. Pochopení příčin a přispívajících faktorů však nemusí být vždy možné nebo nemusí napomáhat neustálému zlepšování bezpečnosti letectví. Očekává se, že tam, kde zranitelnost pramení z aktiv vyvinutých výhradně nebo primárně pro letectví, bude možné provést nezbytné zjištění kořenových příčin. Tyto kořenové příčiny poskytnou dotčené organizaci (organizacím) informaci ke zlepšení procesů a návrhu aktiv s cílem napravit zranitelnost a zajistit, aby taková zranitelnost nebyla zavedena do jiných aktiv. Pochopení kořenových příčin zranitelnosti také umožňuje letecké komunitě získat z tohoto ponaučení a vyhnout se tak podobným zranitelnostem v budoucnu.

GM1 IS.I.OR.215(c) Systém interního hlášení v oblasti bezpečnosti informací

Pokud se toto nařízení vztahuje i na smluvní organizace, výměna informací a hlášení by měly být pokryty v rámci řízení sdílených rizik a prostřednictvím uzavření externí dohody mezi organizacemi.

Pokyny týkající se vytváření externích dohod lze nalézt v dokumentu EUROCAE ED-201A, Chapter 4.4 *External agreements*.

Obecněji a ve všech ostatních případech by každá smlouva o poskytování služeb měla obsahovat standardní doložky týkající se povinností smluvní organizace:

— hlásit v dohodnuté lhůtě incidenty bezpečnosti informací, které mohou mít dopad na organizaci uzavírající smlouvu (zadavatele). Incidenty a zranitelnosti, které by mohly vést k nebezpečným podmínkám, by měly být hlášeny co nejdříve a takovým způsobem, aby bylo možné zajistit externí ohlašovací povinnost podle IS.I.OR.230;

— určit kontaktní místo (osobu) pro správu (řízení) incidentů a případné krizové řízení.

V některých případech smluvní organizace, jako jsou poskytovatelé služeb s distribuovanými zdroji, nemusí být schopny nabídnout žádná ad hoc hlášení. V těchto případech lze požadavek na vnitřní hlášení splnit jinými prostředky, které splňují cíl tohoto ustanovení. Smluvní organizace mohou například poskytnout aktuální seznam zranitelností ovlivňujících systémy v rámci rozsahu smluvních služeb. Tento seznam by měl být organizací uzavírající smlouvu (zadavatelem) sledován jako součást interního hlášení událostí bezpečnosti informací.

GM1 IS.I.OR.215(d) Systém interního hlášení v oblasti bezpečnosti informací

Spolupráce podle bodu IS.I.OR.215(d) může být doložena sdílením prvků ze záznamů incidentů, které mohou podpořit činnosti v oblasti bezpečnosti informací jiných organizací. V případě, že jsou organizace vázány smluvními závazky, může tato smlouva obsahovat i závazek ke spolupráci. Organizace mohou zvážit vytvoření formálních dohod (např. memoranda o porozumění), které vymezují role a odpovědnosti za spolupráci v oblasti bezpečnosti informací, jako jsou schůzky v oblasti správy, společné aktivity v oblasti vývoje a sdílení indikátorů ohrožení – IoC *(indicator of compromise)* v reálném čase.

Kromě toho lze závazku spolupráce dosáhnout také aktivní účastí organizace na iniciativách pro sdílení informací v oblasti bezpečnosti informací; například centra pro sdílení a analýzu informací – ISAC *(information sharing and analysis center)*. Kromě toho se mohou organizace pro vlastní povědomí přihlásit k odběru upozornění na zranitelnosti a hrozby, jako jsou ty, které distribuují CERT.

GM1 IS.I.OR.220 Incidenty bezpečnosti informací – odhalení, reakce a zotavení

Aniž je dotčena definice „události bezpečnosti informací“ v článku 3 nařízení (EU) 2023/203, mezi události, které naznačují potenciální materializaci nepřijatelných rizik, patří obě události (tj. cokoli, co způsobuje škodu nebo má potenciál způsobit škodu) a odhalování zranitelností. Ve skutečnosti jsou rizika informační bezpečnosti spojena s potenciálem, že hrozby zneužijí zranitelnosti, proto je odhalení zneužitelné zranitelnosti událostí bezpečnosti informací.

Ve světle tohoto, v kontextu tohoto nařízení:

— činnosti odhalování požadované podle IS.I.OR.220(a) zahrnují zjišťování zranitelností;

— činnosti reakce požadované podle IS.I.OR.220(b) zahrnují řízení zranitelností.

AMC1 IS.I.OR.220(a) Incidenty bezpečnosti informací – odhalení, reakce a zotavení

ODHALOVÁNÍ

Při plnění požadavku v IS.I.OR.220(a) by měla organizace definovat a zavést strategii pro odhalování incidentů v oblasti bezpečnosti informací, které mohou mít potenciální dopad na bezpečnost.

To by mělo být provedeno tak, aby bylo zajištěno, že je strategie odhalování schopna pokrýt přinejmenším všechny známé hrozby bezpečnosti informací pro jejich aktiva, které se mohou zhmotnit v ohrožení bezpečnosti s nepřijatelnými důsledky.

STRATEGIE ODHALOVÁNÍ

Aby mohla organizace určit rozsah odhalování událostí, měla by:

(a) identifikovat seznam scénářů hrozeb z rizik identifikovaných podle IS.I.OR.205;

(b) identifikovat minimálně ta aktiva, která, jsou-li ohrožena, přispívají ke scénáři (scénářům), který se může zhmotnit v nebezpečném stavu. Pro tuto identifikaci aktiv by měla být rovněž zvážena opatření zavedená podle IS.I.OR.210.

Poznámka: Podíl aktiva na scénáři hrozby a naplnění nebezpečného stavu by měl být posouzen také zvážením celého funkčního řetězce. V některých případech může být aktivum na konci funkčního řetězce, a je-li ohroženo, vliv na bezpečnost je přímý a může být okamžitý; naopak, pokud je aktivum daleko od konce funkčního řetězce a je ohroženo, účinek by se měl šířit a může být opožděn.

GM1 IS.I.OR.220(a) Incidenty bezpečnosti informací – odhalení, reakce a zotavení

STRATEGIE ODHALOVÁNÍ

Při vývoji strategie odhalování pro položky v rozsahu odhalování událostí by měla organizace definovat podmínky, které spouštějí proces, který by například vyžadoval zásah personálu a další analýzu. Tyto podmínky u daných položek lze definovat pomocí prvků z:

(a) očekávané funkční základny: zapojit se do identifikace odchylek od očekávaného funkčního provozu systému (s výjimkou funkcí/kontrol pro bezpečnost informací);

(b) očekávané základny informační bezpečnosti: zapojit se do identifikace odchylek od očekávaného fungování informační bezpečnosti kontrol bezpečnosti informací.

Tyto podmínky by měly brát v úvahu jak abnormální chování, tak podstatné odchylky od výchozích hodnot a relevantní korelaci více nezávislých událostí.

Další pokyny k cílům pro stanovení strategie odhalování lze nalézt v EUROCAE ED-206, Chapter 4.

AMC1 IS.I.OR.220(b) Incidenty bezpečnosti informací – odhalení, reakce a zotavení

(a) INCIDENTY

Organizace by měla při zjišťování souladu s cíli uvedenými v bodě IS.I.OR.220(b) ve vztahu k incidentům vzít v úvahu následující aspekty:

(1) Příprava postupů a vymezení rolí a odpovědností pro včasnou, efektivní a řádnou reakci na jakékoli relevantní incidenty bezpečnosti informací.

(2) Postup reakce by měl:

(i) zvážit varování, jednotlivá nebo kombinovaná, z IS.I.OR.220(a)(2), a ve spolupráci s příslušným personálem posoudit jejich potenciální dopady na bezpečnost letectví;

(ii) stanovit v souladu s IS.I.OR.220(b)(2) strategii izolace *(containment)* pro každou kategorii aktiv s ohledem na možný nejhorší možný účinek a omezení mise a poskytne kritéria, která označují, kdy je incident izolován;

(iii) definovat v souladu s IS.I.OR.220(b)(3) přijatelný dopad na bezpečnost a informační bezpečnost každého aktiva v rozsahu, když selžou v důsledku naplnění scénáře hrozby.

(3) Doba reakce by měla být úměrná úrovni dopadu hodnocené v (2)(iii).

(4) Opatření pro reakci prováděná podle IS.I.OR.220(b) by měla vycházet z postupu reakce uvedeného ve výše uvedeném bodě (a)(2) a měla by zohledňovat zejména následující:

(i) maximální přijatelné snížení úrovně bezpečnosti aktiva v rámci rozsahu incidentu;

(ii) akce, jako je rezistence, izolace, klamání a řízení možných způsobů selhání systémů, které přispějí k dosažení přijatelného snížení úrovně bezpečnosti uvedeného v bodě (i) při minimalizaci dopadu na provoz;

(iii) zdroje potřebné k provádění akcí uvedených v bodě (ii).

(5) Doba a opatření reakce by měly zohledňovat potenciální bezprostřední negativní dopad na bezpečnost, pokud je opatření přijato dříve, než bude plně ověřeno, že nezpůsobí další bezprostřední dopady na bezpečnost.

(b) ZRANITELNÁ MÍSTA (ZRANITELNOSTI)

Organizace by měla při zjišťování souladu s cíli uvedenými v bodě IS.I.OR.220(b) ve vztahu ke zranitelnostem vzít v úvahu následující aspekty:

(1) Stanovení strategie řízení zranitelností definující postupy, role a odpovědnosti, aby bylo možné včas, účinně a řádaně reagovat na jakékoli zjištěné relevantní zranitelnosti.

(2) Opatření pro reakci prováděná podle bodu IS.I.OR.220(b) by měla být založena na maximálním přijatelném riziku položek v rozsahu zranitelnosti s ohledem na nejhorší možný scénář zneužití zranitelnosti.

(3) Doba reakce by měla být úměrná předtriáži při varováních a posouzení potenciálního dopadu zranitelnosti, pokud je zneužita.

GM1 IS.I.OR.220(b) Incidenty bezpečnosti informací – odhalení, reakce a zotavení

Útok je považován za izolovaný (tj. nešíří se dále), pokud byly identifikovány hranice incidentu a hrozba se za tyto hranice nešíří. Další pokyny lze nalézt v dokumentu EUROCAE ED-206 – Chapter 5.

Termín „varování“, jak je používán v IS.OR.220, by měl být chápán jako výstraha, která by vyžadovala včasnou informovanost a reakci týmu pro řízení událostí v oblasti bezpečnosti informací.

V kontextu reakce na bezpečnost informací se „klamání“ týká řady technik, jejichž cílem je uvést v omyl potenciální útočníky nebo uživatele se zlými úmysly, a tím chránit systém a jeho data. Techniky klamání, jako jsou honeypoty nebo drobečková navigace *(breadcrumb trails)*, jsou navrženy tak, aby zmátly, zpomalily nebo odvedly útočníky, zvýšily jejich náklady a riziko a zároveň poskytly obráncům cenný čas a zpravodajské informace.

Poradenský materiál týkající se strategie řízení zranitelnosti lze nalézt v dokumentu EUROCAE ED-206, Chapter 3.4 – *Vulnerability management considerations*. Toto není jediný zdroj, kde lze nalézt návod, a organizace se může odvolávat na jiné poradenské materiály, které jsou pro jejich použití vhodnější.

AMC1 IS.I.OR.220(c) Incidenty bezpečnosti informací – odhalení, reakce a zotavení

Při plnění požadavku v IS.I.OR.220(c) by měla organizace vypracovat postup zotavení se (obnovy) z incidentu zahrnující alespoň následující:

(a) seznam těch aktiv, která umožňují bezpečný provoz, jakož i vzájemné závislosti mezi nimi, tvořící rozsah obnovy;

(b) popis procesu s nezbytnými prioritními akcemi, které mají být provedeny pro návrat aktiv v rozsahu obnovy se do bezpečného a zabezpečeného stavu;

(c) zdroje potřebné k provedení akcí definovaných v bodě (b), aby se zajistilo, že tyto zdroje budou po výskytu incidentu snadno dostupné;

(d) cíle doby obnovy, které by měly být stanoveny ve vztahu ke kritičnosti bezpečnosti aktiv v rozsahu obnovy.

GM1 IS.I.OR.220(b)&(c) Incidenty bezpečnosti informací – odhalení, reakce a zotavení

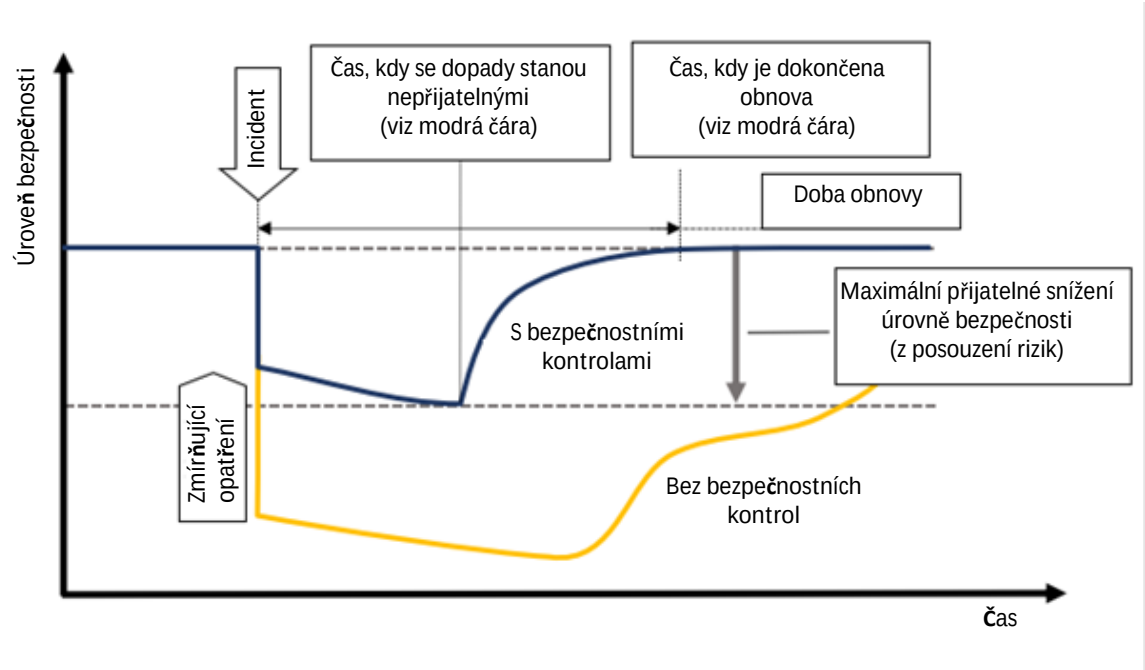
CÍLE A ČASOVÝ ROZVRH OBNOVY

Bod IS.I.OR.220(b) se zabývá podmínkami událostí, které se mohou rozvinout nebo se z nich vyvinuly incidenty bezpečnosti informací, které mohou mít potenciální dopad na bezpečnost letectví, a vyžadují, aby byla zavedena opatření pro reakci a obnovu, s cílem zajistit, že provozní bezpečnost zůstane nad minimální přijatelnou úrovní.

Úroveň provozu a bezpečnosti mohou být vzájemně propojené, takže v některých případech, kdy je úroveň provozu ohrožena incidentem bezpečnosti informací a klesá, úroveň bezpečnosti dělá totéž. To je například případ řízení letového provozu; pokud se letové provozní služby omezí nebo se stanou nespolehlivými, sníží se i bezpečnost letů.

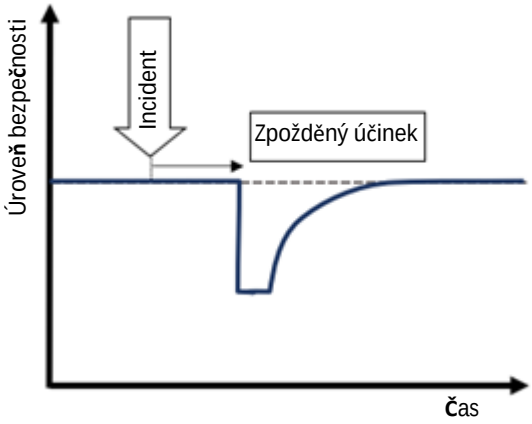
V jiných případech však může být vztah mezi úrovní provozu a bezpečností inverzní, nebo mohou být odděleny, takže když dojde k incidentu a úroveň provozu klesne, úroveň bezpečnosti zůstane zachována. Jedním z příkladů je narušení procesu nahrávání softwaru na palubě letadla. V tomto případě by detekovaný incident následovaný rozhodnutím přerušit operaci nahrávání softwaru zachoval stávající úroveň bezpečnosti.

Následující Obrázek 1 znázorňuje koncepční rámec, který lze vzít v úvahu pro definici cílů reakce a obnovy, včetně doby obnovy. V nejhorším případě představuje, jak se očekávaná úroveň provozní bezpečnosti (úroveň bezpečnosti *(safety level)*) pro proces nebo činnost může měnit v průběhu času, když dojde k incidentu bezpečnosti informací. V tomto scénáři je úroveň bezpečnosti nejprve snížena incidentem, a poté se s plynoucím časem dále snižuje. Obrázek také ukazuje očekávaný účinek, který by měla mít zmírňující opatření a kontroly: v omezení poklesu provozní bezpečnosti, jakmile dojde k incidentu, a ve zlepšení zotavení se (obnovy), tedy návratu na očekávanou úroveň bezpečnosti.

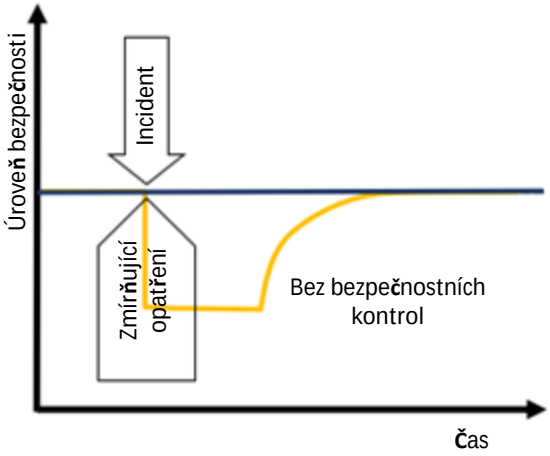


Obrázek 1: Koncepční rámec pro definici cílů reakce a obnovy

Jak již bylo zmíněno, mohou existovat různé vztahy mezi úrovní provozu a bezpečností, které by vedly k odlišnému zobrazení výše uvedeného obrázku. V určitých případech může mít incident zpožděný účinek na úroveň bezpečnosti (např. narušené vývojové prostředí), jak je znázorněno na Obrázku 2, nebo nemusí mít žádný dopad, pokud je řádně kontrolován, jako v případě narušeného procesu nahrávání softwaru uvedeného výše, který je znázorněn na Obrázku 3.



Obrázek 2: Incident se zpožděným účinkem na bezpečnost



Obrázek 3: Incident s plně zmírněným dopadem na bezpečnost

Kromě toho je třeba poznamenat, že mohou existovat různé způsoby, jak lze stejný incident řešit, protože existuje několik faktorů, které mohou ovlivňovat bezpečnost.

V praxi mohou být cíle doby obnovy uvedené v AMC1 IS.I.OR.220(c) vyjádřeny jako seznam zdrojů a služeb, které mají být obnoveny podle pořadí priorit, v rámci rozsahu obnovy. Poradenský materiál týkající se cílů doby obnovy lze nalézt v dokumentu EUROCAE ED-206, Chapter 7.3.5.

GM1 IS.I.OR.220(c) Incidenty bezpečnosti informací – odhalení, reakce a zotavení

Postup zotavení se nebo plán obnovy by měl popisovat činnosti pro zotavení se (obnovu) z incidentu a interní nebo externí zdroje, které jsou dotčeny (např. zaměstnanci, IT, budovy, poskytovatelé). Poradenský materiál týkající se plánu obnovy lze nalézt v dokumentu EUROCAE ED-206, Chapter 7 – *Recover*.

Měly by být k dispozici zdroje potřebné k uplatnění nápravných opatření, aby bylo možné provést nápravná opatření včas poté, co došlo k incidentu. Tyto zdroje mohou být dostupné interně nebo mohou být zajišťovány smluvními organizacemi, jak je stanoveno v IS.I.OR.235. Smlouvy o činnostech obnovy by měly být uzavřeny předtím, než dojde k incidentu (proaktivně), a smlouva by měla obsahovat ujednání, aby smluvní strana mohla včas reagovat.

Návrat do bezpečného a zajištěného stavu může zpočátku vyžadovat nouzová opatření, což jsou činnosti, které jsou zahájeny na základě nejlepších dostupných informací v danou chvíli, než je dosaženo úplného pochopení situace a tato opatření mohou potenciálně snížit úroveň služeb nebo funkcionalit. Návrat do bezpečného a zajištěného stavu by měl být vyhodnocen oproti počátečnímu posouzení rizik a může se pouze dočasně lišit od běžných provozních podmínek. Jakékoli zvýšení zbytkového rizika a trvání tohoto zvýšení rizika, tj. v důsledku provádění mimořádných opatření, by však mělo být zdokumentováno a přijato na správné úrovni odpovědnosti.

Zde uvedené činnosti pro zotavení se (obnovu) mohou být také výsledkem reakce na incidenty, o nichž organizace obdržela informace, že vyžadují provedení odpovídajících opatření, aby reagoval na incidenty nebo zranitelnosti informační bezpečnosti s potenciálním dopadem na bezpečnost letectví.

V takovém kontextu nemusí mít organizace proces nebo plán obnovy pokrývající konkrétní událost. Proto je ze strany organizace obvykle vyžadována definice konkrétního plánu obnovy a jeho schválení příslušným úřadem.

AMC1 IS.I.OR.225 Reakce na nálezy oznámené příslušným úřadem

Vyhovění IS.I.OR.225 by mělo být řízeno tak, jak je pro každou organizaci požadováno v odpovídajícím prováděcím nařízení pro danou oblast, jak je uvedeno v čl. 2 odst. 1 nařízení (EU) 2023/203, co se týče reakce na nálezy oznámené příslušným úřadem. Nařízení pro danou oblast může vyžadovat, aby organizace reagovala na nálezy podle jejich kategorizace.

GM1 IS.I.OR.225 Reakce na nálezy oznámené příslušným úřadem

Požadavek na kategorizaci nálezů a lhůtu, ve které by měly být provedeny kroky v IS.I.OR.225(a), lze nalézt v odpovídajícím prováděcím nařízení pro danou oblast v rámci požadavků na úřady. Při otevření nálezů v souvislosti s tímto nařízením se příslušný úřad bude řídit výše uvedeným požadavkem.

GM1 IS.I.OR.230 Systém externího hlášení v oblasti bezpečnosti informací

Organizace jsou povinny hlásit události svému příslušnému úřadu.

PŘÍKLADY

Projekční organizace schválené EASA: příslušným úřadem je EASA.

Letečtí provozovatelé osvědčení příslušným úřadem členského státu: příslušným úřadem je příslušný úřad členského státu.

ZVLÁŠTNÍ PŘÍPADY

V situaci, kdy má organizace dvě osvědčení leteckého provozovatele (AOC) ve dvou různých členských státech EU (stát A a B), musí být události týkající se letadel provozovaných pod AOC státu A hlášeny příslušnému úřadu státu A; kdežto události týkající se letadel provozovaných pod AOC státu B musí být hlášeny příslušnému úřadu státu B.

U organizací, které mají více oprávnění, bude hlášení podáno příslušnému úřadu schválené části organizace, kde došlo k incidentu nebo kde byla zjištěna zranitelnost. V případě, že incident/zranitelnost ovlivňuje více oprávnění, bude hlášení provedeno všem příslušným úřadům.

Pro organizace, které jsou držiteli oprávnění, ale působí mimo EU (např. podle Části 145), je příslušným úřadem EASA a musí podávat hlášení Agentuře.

Letadla dvojího užití *(dual-use)* – zranitelnost může být nutné hlásit prostřednictvím vojenského i civilního systému hlášení, pokud má vliv na funkci/systém dvojího užití. Informace hlášené prostřednictvím civilního systému hlášení by měly být sanitizovány (tj. všechny citlivé informace by měly být řádně odstraněny).

AMC1 IS.I.OR.230(a)&(b) Systém externího hlášení v oblasti bezpečnosti informací

Aby organizace vyhověla ustanovením podle IS.I.OR.230 (a) a (b), měla by hlásit:

(a) jakoukoli událost, na kterou se vztahuje nařízení (EU) č. 376/2014 a která vznikla úmyslně neoprávněnou elektronickou interakcí;

(b) incidenty bezpečnosti informací s potenciálním významným rizikem pro bezpečnost letectví, na které se nevztahuje nařízení (EU) č. 376/2014;

(c) zranitelnosti, které představují významné riziko pro bezpečnost letectví a nejsou dosud adekvátně zmírněny v souladu se schválenou strategií řízení zranitelností (viz AMC1 IS.I.OR.220(b)).

U výše uvedených hlášení je odpovědností příslušných úřadů podle Části IS zajistit soulad s článkem 7 tohoto nařízení a předložit veškeré relevantní informace, které je třeba sdílet s příslušnými orgány pro bezpečnost informací určenými podle článku 8 směrnice (EU) 2016/1148.

GM1 IS.I.OR.230(a)&(b) Systém externího hlášení v oblasti bezpečnosti informací

VZTAH MEZI IS.I.OR.230(b) A NAŘÍZENÍM (EU) č. 376/2014

Nařízení Evropského parlamentu a Rady (EU) č. 376/2014 stanovuje požadavky na hlášení událostí v civilním letectví, analýzu těchto hlášení a navazující opatření. V\hovění s bodu IS.I.OR.230(b) nezbavuje organizace povinnosti dodržovat nařízení (EU) č. 376/2014.

Pro každou kategorii oznamovatelů definuje nařízení (EU) č. 2015/1018 povahu položek, které mají být povinně hlášeny. Nařízení (EU) č. 376/2014 rovněž uvažuje o dobrovolném hlášení dalších položek, které oznamovatel vnímá jako hrozbu pro bezpečnost letectví.

Kromě toho vyhovění nařízení (EU) č. 376/2014 nezbavuje organizace povinnosti vyhovět bodu IS.I.OR.230(b). Nemělo by to však vést ke vzniku dvou paralelních systémů hlášení a bod IS.I.OR.230(b) a nařízení (EU) č. 376/2014 by se v tomto ohledu měly považovat za vzájemně se doplňující.

V praxi to znamená, že povinnosti hlášení podle bodu IS.I.OR.230(b) na jedné straně a povinnosti hlášení podle nařízení (EU) č. 376/2014 na straně druhé jsou slučitelné. Tyto povinnosti hlášení lze plnit pomocí jednoho kanálu hlášení. Kromě toho může každá fyzická nebo právnická osoba, která má více než jednu roli podléhající povinnosti podat hlášení, splnit všechny tyto povinnosti prostřednictvím jediného hlášení. Organizacím se doporučuje, aby to řádně popsaly ve své organizační příručce, aby se zabývaly případy, kdy jsou odpovědnosti vykonávány jménem organizace.

ANALÝZA NAVAZUJÍCÍCH OPATŘENÍ

Pokud analýza události hlášené podle nařízení (EU) č. 376/2014 později zjistí, že kořenovou příčinou události nebo faktorem přispívajícím k události byla úmyslná neoprávněná elektronická interakce, měla by organizace aktualizovat své oznámení příslušnému úřadu.

VÝZNAMNÉ RIZIKO PRO BEZPEČNOST LETECTVÍ

V souladu s definicí události podle čl. 2 odst. 7 nařízení (EU) č. 376/2014 by jakýkoli incident nebo zranitelnost v oblasti bezpečnosti informací, které mohou představovat významné riziko pro bezpečnost letectví, měly být považovány za událost podléhající hlášení. Významným rizikem pro letectví se rozumí nebezpečný stav, tj. stav, který může vést k nehodě nebo vážnému incidentu (jak je definováno v ICAO Annexu 13).

Poznámka: Při posuzování možnosti, že by účinky incidentu bezpečnosti informací mohly vést k nebezpečnému stavu, by organizace měla zvážit kombinaci účinků, pokud incident zahrnuje více systémů; ve skutečnosti mohou být některé předpoklady o nezávislosti systému, které mohou platit pro náhodné události, úmyslnými činy porušeny.

VZTAH MEZI IS.I.OR.230(b)(1) A JINÝMI POŽADAVKY NA HLÁŠENÍ UDALOSTÍ BEZPEČNOSTI INFORMACÍ SOUVISEJÍCÍCH S LETECKÝMI VÝROBKY NEBO ČÁSTMI

U organizací, na které se vztahují požadavky na hlášení událostí v oblasti bezpečnosti informací souvisejících s leteckými výrobky nebo částmi, se za dostatečné k dosažení vyhovění požadavku v bodě IS.I.OR.230(b)(1) považuje vyhovění specifickým ustanovením prováděcího nařízení pro jejich oblast. Například u organizací, na které se vztahuje nařízení (EU) č. 748/2012, lze hlášení provést v souladu s bodem 21.A.3A Přílohy I (Část 21) uvedeného nařízení.

AMC1 IS.I.OR.230(c) Systém externího hlášení v oblasti bezpečnosti informací

V rámci celkové lhůty 72 hodin by míra naléhavosti pro předložení hlášení měla být určena úrovní dopadu na bezpečnost, o kterém se soudí, že je výsledkem incidentu bezpečnosti informací nebo zjištěné zranitelnosti. Pokud osoba, která identifikuje možný nebezpečný stav, usoudí, že událost vedla k bezprostřednímu a zvláště významnému nebezpečí, příslušný úřad očekává, že bude informován okamžitě a nejrychlejšími možnými prostředky (telefon, fax, e-mail, dálnopis atd.) o všech podrobnostech, které jsou v dané chvíli k dispozici.

GM1 IS.I.OR.230(c) Systém externího hlášení v oblasti bezpečnosti informací

Poradenský materiál týkající se hlášení incidentů a zranitelností bezpečnosti informací lze nalézt v dokumentu EUROCAE ED-206, Chapter 6.4.2.2 – *Reporting timeline* a Chapter 6.4.5 – *Reporting information content*. Toto není jediný zdroj, kde lze nalézt pokyny, a organizace se mohou odvolávat na jiné pokyny, které jsou pro jejich použití vhodnější.

Poznámka: Osoba provádějící hlášení události podle nařízení (EU) č. 376/2014 nemusí být schopna určit povahu události. To platí zejména pro bezpečnost informací a tento výsledek může vycházet z forenzní analýzy, která určuje, že daná události má povahu týkající se bezpečnosti informací. Hodnocení bude provedeno jako součást procesu počátečního interního hlášení (viz IS.I.OR.215 a související AMC). Vyhodnocení události může prokázat možnost, že se zhmotní do nebezpečného stavu s přihlédnutím k pravděpodobnosti realizace.

GM1 IS.I.OR.235 Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací

Organizace se mohou rozhodnout, že určité činnosti zadají dodavatelům, a to jak pro své vlastní provozní potřeby, tak za účelem vyhovění tomuto nařízení (činnosti týkající se řízení bezpečnosti informací). Činnosti nasmlouvané pro provozní potřeby mohou spadat do oblasti působnosti Části IS, a proto musí být příslušná rizika v oblasti bezpečnosti informací řízena v souladu s požadavky v bodech IS.I.OR.205 a IS.I.OR.210. Namísto toho podléhají činnosti týkající se řízení bezpečnosti informací zvláštním ustanovením IS.OR.235, protože záležitosti týkající se těchto činností mohou mít na organizaci významný dopad.

Proto cíle bodu IS.I.OR.235 jsou:

(a) chránit kritické a citlivé informace a aktiva, když s nimi nakládají organizace smluvně zajišťující poskytování činností týkajících se řízení bezpečnosti informací (včetně organizací v dodavatelském řetězci) buď v jejich zařízeních, nebo v zařízeních dané organizace, nebo když jsou přenášeny mezi danou organizací a smluvními organizacemi nebo k nimž mají smluvní organizace vzdálený přístup;

(b) zabránit zavádění rizik v oblasti bezpečnosti informací prostřednictvím produktů a služeb vyvinutých nebo poskytovaných smluvními organizacemi danou organizací v rámci zajišťování činností týkajících se řízení bezpečnosti informací;

(c) zajistit, že jsou rizika v oblasti informační bezpečnosti řízena ve všech fázích vztahu se smluvními organizacemi.

GM2 IS.I.OR.235 Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací

(a) Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací je způsob, jak alokovat úkoly organizace uzavírající smlouvu (zadavatele) na třetí strany (smluvní organizace

(dodavatele)). Organizace uzavírající smlouvu zůstává zodpovědná *(responsible)* za dozor nad smluvní organizací (organizacemi) a odpovědný *(accountable)* za dodržování tohoto nařízení.

(b) Smlouva může mít formu písemné dohody, schvalovacího dopisu, servisního dopisu, memoranda o porozumění atd., jak je pro dané smluvní činnosti vhodné.

GM3 IS.I.OR.235 Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací

PŘÍKLADY

Následující Tabulka 1 uvádí některé příklady činností týkajících se řízení bezpečnosti informací, které mohou být zajišťovány smluvně ve vztahu k ustanovením uvedeným v IS.I.OR.200.

Tabulka 1: Příklady činností týkajících se řízení bezpečnosti informací, které mohou být zajišťovány smluvně

Body IS.I.OR.200, které se vážou k činnostem	Příklad smluvních činností
(a)(1): zavede politiku v oblasti bezpečnosti informací, která stanoví obecné zásady organizace s ohledem na potenciální dopad rizik bezpečnosti informací na bezpečnost letectví;	Návrh politiky informační bezpečnosti a poradenství
(a)(2): identifikuje a přezkoumává rizika bezpečnosti informací v souladu s bodem IS.I.OR.205;	Identifikují aktivity, zařízení a zdroje. Identifikují rozhraní s jinými organizacemi, která by mohla být vystavena rizikům bezpečnosti informací. Provádí analýzu rizik nebo její část, např. identifikuje a klasifikuje rizika informační bezpečnosti.
(a)(3): definuje a provádí opatření k řešení rizik bezpečnosti informací v souladu s bodem IS.I.OR.210;	Definují, vyvíjejí a implementují opatření. Ověřují počáteční a pokračující účelnost implementovaných opatření (např. cvičení červený tým/ modrý tým, penetrační testování, skenování zranitelnosti atd.). Sdělují zúčastněným stranám výsledek posouzení rizik a jejich odpovědnosti v rámci procesu řešení rizik.
(a)(4): provádí systém interního hlášení v oblasti bezpečnosti informací v souladu s bodem IS.I.OR.215;	Definují, vyvíjejí a implementují systém interního hlášení, který umožní shromažďovat a vyhodnocovat události v oblasti bezpečnosti informací a zranitelnosti zařízení, procesů a služeb.
(a)(5): definuje a provádí v souladu s bodem IS.I.OR.220 opatření potřebná k odhalení událostí bezpečnosti informací, identifikuje takové události, které jsou považovány za incidenty s potenciálním dopadem na bezpečnost letectví, s výjimkou případů povolených bodem IS.I.OR.205(e), a reaguje na tyto incidenty bezpečnosti informací a zotavuje se z nich;	Definují, vyvíjejí a implementují opatření k odhalení událostí. Definují, vyvíjejí a implementují opatření, která budou reagovat na podmínky jakékoli události. Definují, vyvíjí a implementují opatření zaměřená na zotavení se z incidentů bezpečnosti informací.
(a)(6): provádí opatření, která byla oznámena příslušným úřadem jako okamžitá reakce na	Implementuje opatření okamžité reakce na incident nebo zranitelnost bezpečnosti informací, jak byla oznámena příslušným úřadem.

Body IS.I.OR.200, které se vážou k činnostem	Příklad smluvních činností
incident nebo zranitelnost bezpečnosti informací s dopadem na bezpečnost letectví;	
(a)(7): přijme v souladu s bodem IS.I.OR.225 vhodné opatření k řešení nálezů oznámených příslušným úřadem;	Identifikuji kořenové příčiny. Definují plán nápravných opatření. Poskytují důkaz o implementovaných nápravných opatřeních pro uzavření nálezu.
(a)(8): provádí systém externího hlášení v souladu s bodem IS.I.OR.230 s cílem umožnit příslušnému úřadu přijmout vhodná opatření;	Definují, vyvíjejí a implementují systém externího hlášení, který umožní sdělování informací o incidentech v oblasti bezpečnosti informací a zranitelnosti zařízení, procesů a služeb příslušnému úřadu a v případě potřeby držiteli schválení návrhu nebo organizaci odpovědné za návrh.
(a)(9): splňuje požadavky uvedené v bodě IS.I.OR.235 při uzavírání smluv na jakoukoli část činností uvedených v bodě IS.I.OR.200 s jinými organizacemi;	Nepoužitelné
(a)(10): splňuje požadavky na personál stanovené v bodě IS.I.OR.240;	Činnosti odpovědného vedoucího v rámci ustanovení pro „společnou odpovědnou osobu“, jak je uvedeno v IS.I.OR.240. Sledování shody, jak předpokládá IS.I.OR.240. Smluvní organizace k zajištění, že je k výkonu činností souvisejících s tímto nařízením ve službě dostatek personálu. Definují, vyvíjejí a poskytují adekvátní školení k dosažení kompetencí, které jsou u personálu požadovány. Provádí kontroly před nástupem do zaměstnání.
(a)(11): splňuje požadavky na vedení záznamů stanovené v bodě IS.I.OR.245;	Definují, vyvíjejí a implementují zabezpečenou archivaci. Poskytování zabezpečeného datového centra (jako služby) Poskytování aktualizací záznamů
(a)(12): sleduje soulad organizace s požadavky tohoto nařízení a poskytuje zpětnou vazbu v souvislosti s nálezy odpovědnému vedoucímu za účelem zajištění účinného provádění nápravných opatření;	Sledování shody (jak předpokládá IS.I.OR.240), včetně provádění nezávislých auditů.
(a)(13): chrání, aniž jsou dotčeny příslušné požadavky na hlášení incidentů, důvěrnost veškerých informací, které organizace případně obdržela od jiných organizací, podle úrovně jejich citlivosti.	Definují, vyvíjejí a implementují řešení na ochranu důvěrnosti jakýchkoli informací.
(b): Aby neustále splňovala požadavky uvedené v článku 1, organizace provádí proces neustálého zlepšování v souladu s bodem IS.I.OR.260.	Provádějí nezávislé hodnocení účelnosti a vyspělosti. Definují, vyvíjejí a implementují nezbytná opatření ke zlepšení.
(c): Organizace v souladu s bodem IS.I.OR.250 dokumentuje všechny klíčové procesy, postupy, úlohy a povinnosti požadované za účelem dosažení souladu s bodem IS.I.OR.200(a) a	Vypracování dokumentace s podrobnými informacemi o všech klíčových procesech, postupech, rolích a odpovědnostech vyžadovaných pro splnění bodu IS.I.OR.200(a)

Body IS.I.OR.200, které se vážou k činnostem	Příklad smluvních činností
zavede proces pro změnu uvedené dokumentace. Změny uvedených procesů, postupů, úloh a povinností se řídí podle bodu IS.I.OR.255.	(např. zásad bezpečnosti informací, obecného popisu personálu, postupů pro specifikaci vyhovění). Definují, vyvíjejí a implementují procesy pro schvalování dodatků a změn.

AMC1 IS.I.OR.235(a) Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací

(a) DOZOR NAD SMLUVNÍ ORGANIZACÍ

Aby mohla daná organizace vykonávat dozor nad smluvní organizací, měla by mít:

(1) proces, který zajistí vyhovění ustanovením v tomto nařízení týkajících se smluvních činností;

(2) strukturovaný proces sledující očekávané plnění smlouvy, který zahrnuje:

(i) vymezení a odsouhlasení rozsahu činností;

(ii) definici rolí a odpovědností stran (tj. organizace uzavírající smlouvu (zadavatele) a smluvní organizace (dodavatele));

(iii) definici a přezkum ukazatelů KPI;

(iv) reakci na odchylku od smluvních závazků;

(v) provádění auditů shody, podle předem definovaného rozsahu a cílů, s cílem vyhodnotit provozní a související zabezpečovací činnosti;

(vi) poskytování zpětné vazby o výsledcích auditů shody jak v rámci dané organizace, tak smluvní organizaci a reakce na nálezy. Zpětná vazba o výsledku auditů shody v rámci organizace uzavírající smlouvu by se měla dostat k odpovědnému vedoucímu nebo delegované osobě (osobám), aby bylo zajištěno řádné sledování reakce na nálezy (tj. provedení nápravných opatření), nebo bude-li to považováno za nutné, ukončení smlouvy.

Poznámka: Právo dané organizace provádět audity shody smluvní organizace by mělo být zahrnuto ve smlouvě mezi těmito stranami.

(b) ŘÍZENÍ RIZIK SPOJENÝCH SE SMLUVNÍMI ČINNOSTMI

Aby mohla řádně řídit rizika spojená se smluvními činnostmi, měla by organizace splňovat tato kritéria:

(1) Před outsourcingem jakýchkoli činností týkajících se řízení bezpečnosti informací se provádí předchozí posouzení dodavatelů. Posouzení by mělo hodnotit kompetence dodavatelů, jejich udržitelnost a kvalifikace ve vztahu k činnostem, které mají být smluvně zajišťovány.

(2) Dochází k posuzování rizik spojených s poskytováním smluvních činností, které bylo dohodnuto mezi danou organizací podle Části IS a smluvní organizací.

(3) Organizace zřizuje a udržuje vhodné komunikační kanály pro bezpečnost informací se smluvní organizací.

GM1 IS.I.OR.235(a) Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací

PŘEDCHOZÍ POSOUZENÍ

Účelem předchozího posouzení je vyhodnotit kompetence, udržitelnost a kvalifikace dodavatelů ve vztahu k činnostem v oblasti bezpečnosti informací, které mají být smluvně zajišťovány. Toto předchozí posouzení může být nutné provést s přihlédnutím k dalším právním požadavkům nebo postupům zadávání zakázek, které se na organizaci vztahují, a může být proto provedeno různými způsoby, jako například:

(a) v případě veřejných nabídek zahrnutí požadavků způsobilosti do zadávací dokumentace pro potenciální dodavatele;

(b) přezkoumání certifikací bezpečnosti informací potenciálním dodavatelům udělených externími a nestrannými auditory;

(c) přezkoumání sebehodnotících dotazníků sestavených potenciálními dodavateli.

POSOUZENÍ RIZIK SPOJENÝCH S POSKYTOVÁNÍM SMLUVNÍCH ČINNOSTÍ

Posouzení rizik by mělo vzít v úvahu úroveň vyspělost smluvní organizace a mělo by vzít v úvahu následující:

(a) identifikaci a posouzení kritických a citlivých informací a aktiv, které mohou být s externími dodavateli sdíleny nebo které mohou být externími dodavateli poskytovány;

(b) identifikaci požadavků dané organizace na bezpečnost informací, které se vztahují na smluvní organizaci;

(c) hodnocení schopnosti smluvní organizace (stávající i nové smluvní organizace) plnit požadavky organizace uzavírající smlouvu (zadavatele) na bezpečnost informací, a to prostřednictvím posouzení dodavatele;

(d) posouzení rizik, které může smluvní organizace přinést.

Toto odsouhlasené posouzení rizik by také mělo vzít v úvahu role a odpovědnosti organizace uzavírající smlouvu (zadavatele) a smluvní organizace (dodavatele) a také jejich rozhraní.

GM2 IS.I.OR.235(a) Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací

AUDIT SMLUVNÍCH ORGANIZACÍ

Při auditování dodavatele, se kterým má uzavřenu smlouvu na provádění činností řízení bezpečnosti informací, by měla organizace vzít v úvahu následující aspekty:

— rozsah auditu, jakož i cíl by měly být omezeny na procesy, zdroje (tj. personál smluvní organizace, systémy/vybavení, sítě) a data používaná k provádění smluvních činností podle Části IS;

— audity shody a/nebo implementace by měly být prováděny podle uvážení organizace uzavírající smlouvu (zadavatele);

— nálezy zjištěné během auditu by měly být řešeny prostřednictvím plánu nápravných opatření spolu s časovým rámcem, které má organizace uzavírající smlouvu (zadavatel) potvrdit.

AMC1 IS.I.OR.235(b) Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací

Aby zajistila na vyžádání přístup příslušného úřadu do smluvní organizace, měla by organizace podle Části IS zajistit, že jsou takový požadavek nebo ustanovení zahrnuty do smluvní dokumentace.

Přístup příslušného úřadu do smluvních organizací by měl být přinejmenším rovnocenný přístupu udělenému organizaci uzavírající smlouvu (zadavateli) a v každém případě by měl být dostatečný k zajištění posouzení trvalého souladu smluvních činností s platnými požadavky.

GM1 IS.I.OR.235(b) Uzavírání smluv na činnosti týkající se řízení bezpečnosti informací

Přístup do smluvní organizace znamená mít možnost vidět důkaz vyhovění smluvních činností (jako jsou artefakty, dokumenty, nezávislé certifikace).

Důkazu vyhovění lze dosáhnout buď předáním dokumentů a/nebo přístupem k informacím v prostorách v souladu s „rozsahem auditu“, jak je definován ve smlouvě.

V těch případech, kdy by organizace využívala komerční běžné služby se standardními smluvními doložkami jako součást nasmlouvaných činností týkajících se řízení bezpečnosti informací, měla by organizace zvážit, zda tyto doložky poskytují dostatečný přístup k požadovaným informacím.

Možnost navštívit prostory by měla být vyhodnocena s ohledem na různé aspekty, jako je citlivost souvisejících informací nebo praktická dostupnost smluvní organizace (např. smluvní organizace je poskytovatel služeb s distribuovanými zdroji).

GM1 IS.I.OR.240 Požadavky na personál

Cíle požadavků obsažených v bodech (a) až (e) jsou:

(a) zajistit, že je zavedena účinná organizační struktura, aby byly splněny požadavky tohoto nařízení;

(b) zajistit důvěru v ostatní organizace, se kterými sdílejí rizika.

AMC1 IS.I.OR.240(a)(2) Požadavky na personál

PODPORA POLITIKY BEZPEČNOSTI INFORMACÍ

Odpovědný vedoucí dané organizace by se měl ujistit, že politika bezpečnosti informací je zaměstnancům známa a snadno přístupná, a to přiměřeně jejich povinnostem.

AMC1 IS.I.OR.240(a)(3) Požadavky na personál

ZÁKLADNÍ POROZUMĚNÍ NAŘÍZENÍ

Aby bylo možné prokázat základní porozumění tomuto nařízení, odpovědný vedoucí organizace by měl být schopen vysvětlit zastřešující cíle tohoto nařízení a jeho důsledky pro organizaci.

GM1 IS.I.OR.240(a)(3) Požadavky na personál

ZÁKLADNÍ POROZUMĚNÍ NAŘÍZENÍ

V případě, že odpovědný vedoucí nemá žádné předchozí zkušenosti v oblastech činností souvisejících s Částí IS, může získat potřebné znalosti tím, že se zúčastní školení zahrnujícího obsah tohoto nařízení a technický základ pro vyhovění (shodu). Školicí materiál by měl zejména pokrývat zastřešující cíle Části IS a hodnocení by mělo posoudit porozumění těmto regulatorním cílům.

AMC1 IS.I.OR.240(b) Požadavky na personál

JMENOVÁNÍ OSOBY NEBO SKUPINY OSOB

Osoba nebo skupina osob jmenovaná podle bodu IS.I.OR.240(b) se zodpovědností *(responsibility)* zajistit vyhovění požadavkům tohoto nařízení by měla představovat řídící strukturu organizace.

Tato osoba nebo skupina osob má přímý přístup k odpovědnému vedoucímu (nebo společné odpovědné osobě, je-li jmenována), aby zajišťovala vedení, směr a podporu plánování, implementaci a fungování procesu a standardů, aby byly v souladu s nařízením. Měli by mít přímý přístup k tomu, aby odpovědného vedoucího (nebo společnou odpovědnou osobu) řádně informovali o záležitostech shody a bezpečnosti informací (například prostřednictvím setkání organizovaných na pravidelné bázi).

Jmenování by mělo zohledňovat možnost, že osoba nemusí být po určitou dobu schopna plnit jí přidělené organizační úkoly, a tedy také určit potřebné zástupce.

Tyto jmenované osoby by měly prokázat plné porozumění požadavkům tohoto nařízení, aby byly schopny zajistit, že procesy a standardy organizace přesně reflektují použitelné požadavky. Jejich úlohou je zajistit, aby byla shoda proaktivně řízena a aby byly zdokumentovány všechny rané varovné signály neshody a aby se podle toho jednalo.

Popis funkcí a zodpovědností jmenovaných osob a zástupců, včetně jejich jmen, by měl být obsažen v ISMM (viz bod IS.I.OR.250(a)(2)).

GM1 IS.I.OR.240(b) Požadavky na personál

Podmínka dlouhodobé nepřítomnosti jmenované osoby nastává, když tato osoba není schopna plnit svěřené organizační povinnosti. Je-li například požadováno, aby činnost týkající se řízení bezpečnosti informacíí vykonávaly jmenované osoby ve stanoveném intervalu, nepřítomnost se považuje za dlouhodobou, pokud tento interval překročí, a proto může dojít ke zranitelnosti v činnosti řízení.

GM1 IS.I.OR.240(b)&(c) Požadavky na personál

Jmenování lze provést prostřednictvím e-mailu, organizačního schématu, tabulky rolí a zodpovědností atd., které organizace obvykle používá. Organizace může přijmout pro výše uvedené pozice řízení bezpečnosti informací jakékoli názvy, ale měla by příslušnému úřadu identifikovat názvy a osoby vybrané k výkonu těchto funkcí.

GM1 IS.I.OR.240(c) Požadavky na personál

FUNKCE SLEDOVÁNÍ SOULADU (SHODY)

Osoba jmenovaná podle bodu IS.I.OR.240(c) se zodpovědností za řízení funkce sledování souladu (shody) požadované podle bodu IS.I.OR.200(a)(12) může být stejná osoba jako osoba odpovědná za funkci sledování souladu (shody) vyžadovaná prováděcím předpisem pro danou oblast, nebo ji může informovat.

AMC1 IS.I.OR.240(d) Požadavky na personál

KOORDINACE

Kritéria pro zavedení koordinace, která zajistí adekvátní integraci řízení bezpečnosti informací v rámci organizace, jsou následující:

(a) rozsah a hranice organizací byly stanoveny a sděleny společné odpovědné osobě;

(b) požadavky tohoto nařízení byly sděleny společné odpovědné osobě a sdíleny s ní;

(c) společná odpovědná osoba má přímý přístup k odpovědnému vedoucímu;

(d) problémy jsou proaktivně řízeny a jakékoli rané varovné signály neshody jsou dokumentovány a jedná se podle toho.

GM1 IS.I.OR.240(e) Požadavky na personál

SPOLEČNÁ ODPOVĚDNÁ OSOBA

Je-li odpovědným vedoucím pro činnosti podle tohoto nařízení pověřena společná odpovědná osoba (CRP), mělo by být této osobě rovněž přiděleno příslušné pověření, které je nezbytné k tomu, aby implementovala ustanovení IS.I.OR.200, včetně pravomocí a finančních prostředků k mobilizaci a řízení zdrojů napříč organizacemi nebo částmi dotčené organizace. Toto pověření může rovněž zahrnovat jmenování osoby nebo skupiny osob uvedených v IS.I.OR.240(b) a (c) a obecně může CRP při plnění jeho/jejích povinností pomáhat další personál.

Možnost pověření CRP se vztahuje na organizaci, která 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, a proto se očekává, že tato CRP bude mít zodpovědnosti a kompetence v oblasti informační bezpečnosti. Zejména by CRP měla být schopna řídit strategii bezpečnosti informací úřadu a její implementaci, aby bylo zajištěno dosažení cílů popsaných v článku 1. Podle Evropského rámce dovedností v oblasti kybernetické bezpečnosti – *European Cybersecurity Skills Framework* (ECSF) zveřejněného agenturou ENISA v září 2022 může být tato osoba popsána například jako: (vedoucí) manžer informační bezpečnosti ((C)ISO), ředitel programu pro kybernetickou bezpečnost nebo manažer pro bezpečnost informací. Je však třeba poznamenat, že tyto popisy a související dovednosti nezohledňují hledisko bezpečnosti letectví požadované v článku 1.

Pokud je subjekt držitelem více oprávnění nebo prohlášení, mohou příslušní odpovědní vedoucí pověřit stejnou CRP, která tedy bude zodpovědná za implementaci ustanovení IS.I.OR.200 pro funkční cluster sdílející struktury, politiky, procesy a procedury v oblasti bezpečnosti informací.

AMC1 IS.I.OR.240(f) Požadavky na personál

DOSTATEČNÝ POČET PRACOVNÍKŮ

Pro určení dostatečnosti personálu je třeba vzít v úvahu následující prvky:

(a) organizační struktury, zásady, procesy a postupy podléhající řízení bezpečnosti informací;

(b) rozsah požadované koordinace s ostatními organizacemi, kontraktory a dodavateli;

(c) míru rizika spojeného s organizací vykonávanými činnostmi.

GM1 IS.I.OR.240(f) Požadavky na personál

DOSTATEČNÝ POČET PRACOVNÍKŮ

Pro účely tohoto nařízení se personálem rozumí kombinace pracovníků přímo zaměstnaných organizací a smluvního personálu, jak je uvedeno v IS.I.OR.235.

Činnosti uvedené v Dodatku II, týkající se hlavních úkolů vyplývajících z provádění Části IS, by měly být zohledněny při vytváření organizační struktury nezbytné pro splnění požadavků tohoto nařízení.

AMC1 IS.I.OR.240(g) Požadavky na personál

NEZBYTNÁ ZPŮSOBILOST (KOMPETENCE)

(a) Pro určení způsobilosti (kompetence) potřebné u personálu provádějící tyto činnosti by měly být vzaty v úvahu následující prvky:

(1) pracovní role a související úkoly;

(2) požadované znalosti, dovednosti a schopnosti.

(b) V rámci procesu, který má zajistit, aby si pracovníci zachovali nezbytnou způsobilost (kompetenci), by měla organizace:

(1) posoudit kvalifikaci a praxi personálu s ohledem na požadovanou způsobilost (kompetenci) pro přidělené pracovní role s cílem identifikovat mezery (slabá místa);

(2) sladit kvalifikaci a praxi personálu s očekávanou způsobilostí (kompetencí) plnit své role organizováním odpovídajících vzdělávacích programů pro stávající členy personálu, náborem nových zdrojů nebo jejich kombinací;

(3) udržovat způsobilost (kompetence) personálu po dobu, po kterou jsou zařazeni do pracovní role.

GM1 IS.I.OR.240(g) Požadavky na personál

NEZBYTNÁ ZPŮSOBILOST (KOMPETENCE) A PROGRAM VÝCVIKU

Program výcviku by měl začínat identifikací způsobilosti (kompetence) vyžadované u personálu pro každou roli, následovanou identifikací mezer (slabých míst) mezi způsobilostí (kompetencí) stávající a požadovanou.

Za účelem vytvoření seznamu způsobilostí (kompetencí) může organizace použít jako počáteční vodítko stávající rámec kompetencí v oblasti kybernetické bezpečnosti, jako je NICE *(National Initiative for Cybersecurity Education)* založený na rámci kybernetické bezpečnosti NIST – *NIST Cybersecurity Framework* (NIST CSF).

V Dodatku II jsou uvedeny hlavní úkoly tohoto nařízení a namapovány na způsobilosti (kompetence) odvozené od NIST CSF. Toto mapování lze použít k vytvoření základní linie pro identifikaci výše uvedených mezer (slabých míst) ve způsobilostech (kompetencích). Je však třeba poznamenat, že stávající rámce způsobilosti (kompetencí) v oblasti kybernetické/informační bezpečnosti, jako je NICE, se obvykle zaměřují především na ochranu standardních informačních technologií; navrhovaný seznam způsobilostí (kompetencí) proto může být nutné přizpůsobit technologiím nebo integrovat do procesů, které jsou používány v organizaci.

Překlenutí zjištěných mezer (slabých míst) by mělo být chápáno jako cíl programu výcviku, který by měl dále zahrnovat rozsah, obsah, metody poskytování (např. školení v učebně (classroom), e-learning, notifikace, zácvik na pracovišti (OJT)) a četnosti školení, které nejlépe odpovídají potřebám organizace s ohledem na velikost, rozsah, požadované kompetence a složitost organizace.

A konečně, jak se informační/kybernetická bezpečnost vyvíjí v důsledku nárůstu nových hrozeb, měla by organizace adekvátnost programu výcviku pravidelně přezkoumávat.

AMC1 IS.I.OR.240(h) Požadavky na personál

UZNÁNÍ POVINNOSTÍ

Pokud jde o jakoukoli přidělenou roli a úkol, organizace by měla jasně a transparentně specifikovat všechny odpovědnosti za bezpečnost informací, které má zaměstnanec.

V rámci toho by všichni pracovníci vykonávající činnosti požadované tímto nařízením měli dohledatelným a ověřitelným způsobem potvrdit, že rozumí přiděleným rolím a souvisejícím povinnostem (odpovědnostem) v oblasti bezpečnosti informací.

GM1 IS.I.OR.240(h) Požadavky na personál

UZNÁNÍ POVINNOSTÍ

Potvrzení o přijetí, jako je platný elektronický podpis nebo vlastnoruční podpis na papíře, potvrzovací e-mail atd., je dohledatelným důkazem potvrzení.

AMC1 IS.I.OR.240(i) Požadavky na personál

TOTOŽNOST A DŮVĚRYHODNOST

U personálu, který má přístup k informačním systémům a datům podléhajícím požadavkům Části IS, by měla být identita určena na základě listinných důkazů.

K prokázání důvěryhodnosti tohoto personálu by organizace měla mít zdokumentovaný proces a vhodná kritéria, která zajistí, že jednotlivcům je možné při výkonu jejich role důvěřovat.

GM1 IS.I.OR.240(i) Požadavky na personál

TOTOŽNOST A DŮVĚRYHODNOST

(a) Důvěryhodnost lze prokázat například:

(1) před nástupem do zaměstnání – ověřením spolehlivosti provedeném v souladu s platnými předpisy unijního a vnitrostátního práva. Toto ověření může zahrnovat verifikaci:

(i) vzdělání, předchozích zaměstnání a případných mezer v předchozích letech;

(ii) absence záznamu v rejstříku trestů;

(iii) jakékoli další relevantní informace nebo zpravodajské informace považované za relevantní pro vhodnost osoby pro práci v předpokládané roli;

(2) v průběhu zaměstnání – sledování věrnosti závazkům a chování zaměstnance.

Poznámka: Absenci záznamu v rejstříku trestů lze ověřit prostřednictvím osvědčení vydaného odpovědným orgánem v členském státě v souladu s nařízením (EU) 2016/1191. V případě potenciálních zahraničních zaměstnanců mohou být výše uvedená ověření prováděna na základě rovnocenných osvědčení vydaných zemí původu, jako je „výpis z rejstříku trestů *(certificate of good conduct)*“.

(b) V případě procesu a kritérií pro stanovení důvěryhodnosti personálu bude možná potřeba dále zvážit, zda:

(1) informační systémy a data, ke kterým se má přistupovat, se při procesu posouzení rizik podle IS.I.OR.205 pojily s vysokou závažností bezpečnostních důsledků;

(2) kontroly nebo zmírňující opatření k řešení rizik identifikovaných během analýzy rizik závisí na organizačních/provozních postupech – například na správné konfiguraci a správě informačních technologií, databázových operacích, monitorování bezpečnosti informací atd.

V takových případech může personál, který má práva administrátora nebo nekontrolovaný a neomezený přístup k systémům a datům uvedeným výše v bodě (a)(1), nebo personál, který uplatňuje opatření podle výše uvedeného bodu (b)(2), podléhat přísnějším kritériím.

(c) Zpravodajské a jakékoli další relevantní informace lze shromažďovat prověřováním a analýzou veřejných zdrojů, jako jsou sociální média a webové stránky, v rámci mezí stanovených příslušnými vnitrostátními zákony a předpisy.

(d) Na některé organozace podle Části IS se také může vztahovat nařízení (EU) 2015/1998, které vyžaduje u personálu v určitých rolích úspěšné absolvování ověření spolehlivosti, jakož i mechanismus pro průběžný přezkum těchto ověření. V takových případech může organizace

k prokázání totožnosti a důvěryhodnosti personálu požadovaných v Části IS, ve vztahu k jejich roli, za vhodné považovat proces a příslušná kritériím definované v nařízení (EU) 2015/1998 pro standardní a důkladnější ověření spolehlivosti. Je však třeba poznamenat, že vyhovění požadavkům na prokázání totožnosti a důvěryhodnosti podle Části IS nepředstavuje vyhovění požadavkům na ověření spolehlivosti, jak jsou definovány v nařízení (EU) 2015/1998.

GM1 IS.I.OR.245 Vedení záznamů

Záznamy jsou vyžadovány k dokumentaci dosažených výsledků nebo k doložení provedených činností. Záznamy se po zaznamenání stávají faktickými a nelze je upravovat. Proto nepodléhají kontrole verzí. I když je vytvořen nový záznam týkající se stejného problému, předchozí záznam zůstává platný.

„Obdržená oprávnění“ uvedená v bodě (a)(1)(i) zahrnují jakékoli „osvědčení“, které organizace obdržela, pokud je to stanoveno prováděcím pravidlem pro její doménu.

AMC1 IS.I.OR.245(a)(1)(vi)&(a)(5) Vedení záznamů

Při plnění požadavků podle bodů (a)(1)(vi) a (a)(5) by organizace měla zavést politiku uchovávání dat definující postupy pro:

(a) správu příslušných souborů dat bezpečnosti informací;

(b) stanovení pravidelného posouzení jejich obsahu; a

(c) definování kritérií umožňujících vymazání záznamů o událostech bezpečnosti informací, pokud byl splněn cíl požadavku (a)(5).

GM1 IS.I.OR.245(a)(1)(vi)&(a)(5) Vedení záznamů

Cílem požadavku (a)(1)(vi) je zajistit detekci možného náznaku incidentů nebo zranitelností v oblasti bezpečnosti informací, které nejsou zřejmé při běžném provozu (např. dříve neznámé situace), zatímco cílem požadavku podle (a)(5) je umožnit nezbytnou flexibilitu při řízení objemu uložených událostí bezpečnosti informací.

Záznamy o událostech bezpečnosti informací zahrnují ty události, které byly identifikovány v rámci detekčních činností podle IS.I.OR.220(a), jakož i další data bezpečnosti informací vytvořená aktivy, která byla identifikována podle IS.I.OR.205.

Politika uchovávání dat objasňuje, jaké informace by měly být uchovávány nebo archivovány a jak dlouho. Některé pokyny k uchovávání dat lze nalézt v dokumentu EUROCAE ED-206, Chapter 2.6.

Jakmile dataset dokončí dobu uchovávání, lze jej smazat nebo přesunout jako trvalá historická data do sekundárního nebo terciárního úložiště.

AMC1 IS.I.OR.245(c)&(d) Vedení záznamů

Při plnění požadavků podle bodů (c) a (d) pro všechny záznamy požadované v bodech IS.I.OR.245 (a) a (b) by organizace měla zvážit následující:

(a) Záznamy by měly být uchovávány v papírové podobě nebo v elektronické podobě nebo v kombinaci obou médií. Záznamy by měly zůstat přístupné, kdykoli je to potřeba, v přiměřené době a použitelné po celou požadovanou dobu uchovávání. Doba uchovávání začíná okamžikem vytvoření záznamu.

(b) Integrita, dostupnost a autenticita dat záznamů by měla být chráněna v souladu s ochranou odpovídajících provozních dat a jako taková by měla spadat do působnosti ISMS.

(c) Úložné systémy by měly být chráněny před neoprávněným přístupem (tj. pokusy o únik dat osobních údajů/úpravy záznamů), a proto by měly mít implementována opatření pro bezpečnost informací v souladu s úrovní rizika bezpečnosti informací, které je s nimi spojeno.

(d) Jakmile již záznamy nemusí být uchovávány, mělo by být náležitě provedeno zničení záznamů a vyřazení majetku používaného k jejich uložení.

GM1 IS.I.OR.245(c)&(d) Vedení záznamů

PŘÍSTUPNOST ZÁZNAMŮ PO CELOU DOBU UCHOVÁVÁNÍ

Doporučuje se dodržovat osvědčené postupy pro uchovávání dat, v případě dat, která může být nutné obnovit, strategie zálohování, jako je použití automatických nástrojů zálohování, segregaci nebo geografickou separaci míst úložišť záloh, a zvážit offline zálohování s cílem zabránit rizikům ransomwaru. Tyto postupy by měly být zváženy také tehdy, když je vedení záznamů smluvně zajištěno poskytovateli služeb s distribuovanými zdroji.

Zvláštní pozornost by měla být věnována významným změnám hardwaru a softwaru, aby se zajistilo, že uložené digitální záznamy zůstanou přístupné a čitelné (např. systém souborů, formát souborů aplikace, dopředně kompatibilní verze databáze atd.). Papírové informace je třeba archivovat v adekvátním prostředí, ve kterém jsou záznamy chráněny před degradačními faktory (např. nadměrným teplem, světlem nebo vlhkostí).

INTEGRITA DAT ZÁZNAMŮ A OCHRANA PROTI NEOPRÁVNĚNÉMU PŘÍSTUPU

Běžně používanou metodou k dosažení ochrany autenticity a integrity je použití digitálních podpisů na úrovni dokumentu. Do souboru dokumentu (např. PDF) lze přidat digitální podpisy, aby bylo zajištěno, že záznam nebyl upraven někým jiným než jeho autorem (integrita) a že autor je, kdo se očekává, že má být (autenticita).

Kromě toho, aby se zabránilo neoprávněnému přístupu, lze záznamy chránit například implementací metody řízení přístupu na základě role – *role-based access control* (RBAC) nebo lze určité záznamy chránit heslem na úrovni souborů. Komerční aplikace obsahují vestavěné základní funkce ochrany heslem pro jejich formáty souborů. Ochrany přístupu lze také dosáhnout ochranou prostředí, kde jsou jednotlivé záznamy uloženy (např. ochrana přístupu k databázím, sdíleným souborům, adresářům atd.).

GM1 IS.I.OR.250(a) Příručka pro řízení bezpečnosti informací (ISMM)

Organizace se může rozhodnout dokumentovat některé informace požadované podle bodu IS.I.OR.250(a) v samostatných dokumentech (např. postupy). V tomto případě by měla zajistit, aby příručka obsahovala odpovídající odkazy na jakýkoli dokument uchovávaný samostatně. Všechny takové dokumenty je pak třeba považovat za nedílnou součást příručky systému řízení bezpečnosti informací organizace.

V případě, že je subjekt držitelem více oprávnění nebo prohlášení, může ISMM platit pro jednu nebo více organizací současně na základě společného ISMS. Tato ISMM by měla obsahovat alespoň schvalovací dokument každé organizace a měla by být formálně schválena odpovědným vedoucím nebo odpovědnou osobou každé organizace. Společná odpovědná osoba může být jmenována podle IS.I.OR.240(d) a pokynů GM1 IS.I.OR.240(e).

Aby bylo zajištěno, že všechny zúčastněné strany mohou plnit své povinnosti, doporučuje se, aby všechny příručky, postupy a komunikace mezi nimi byly přinejmenším v jednom společném jazyce, např. angličtině. Mezi tyto zúčastněné strany patří příslušné úřady, s nimiž by měl být společný jazyk dohodnut.

AMC1 IS.I.OR.255 Změny systému řízení bezpečnosti informací

Aniž je dotčeno oznamování změn, jak je požadováno pro každou organizaci v odpovídajícím prováděcím nařízení pro oblast uvedenou v čl. 2 odst. 1 nařízení (EU) 2023/203, postup uvedený v IS.I.OR.255(a)(1) by měl při navrhování způsobu, jakým budou řízeny, zohledňovat kritičnost daných změn. Zejména ty změny, které by mohly mít dopad na dosažení nebo udržení souladu s ustanoveními Části IS nebo které by mohly vést k nepřijatelné úrovni rizika (např. podle pokynů uvedených v GM1 IS.I.OR.205(c)), by měly být podrobeny kontrole. Po zavedení tohoto postupu by jakékoli jeho další změny měly podléhat schválení příslušným úřadem.

Pokud je požadováno předchozí schválení od příslušného úřadu pro změnu, na kterou se nevztahuje schválený postup, nebo pokud takový schválený postup neexistuje, měla by organizace poskytnout alespoň tyto informace:

— povaha a účel změny;

— plán implementace změny;

— plán ověření změny;

— potenciální dopad na bezpečnost letectví, který změna přináší.

Významná odchylka od původního plánu implementace během procesu změny je událost, která by měla být hlášena příslušnému úřadu, protože tato odchylka může vyžadovat přehodnocení dopadu změny.

GM1 IS.I.OR.255 Změny systému řízení bezpečnosti informací

Bod IS.I.OR.255 má následující strukturu:

Bod (a) zavádí možnost, aby se organizace dohodla s příslušným úřadem, že změny ISMS mohou být implementovány bez předchozího schválení, pokud se na tyto změny vztahuje postup pro změny.

Bod (b) zavádí povinnost předchozího schválení (příslušným úřadem) v případě změn, na které se nevztahuje výše uvedený postup, a uvádí, jak by mělo být s těmito změnami naloženo.

Organizace by měla zvážit zavedení postupu pro řízení a oznamování změn příslušnému úřadu, jak je stanoveno v IS.I.OR.255(a). V případě neexistence jakéhokoli schváleného postupu bude muset organizace pro jakoukoli změnu požádat o schválení a získat jej, jak je požadováno v IS.I.OR.255(b). V každém případě by všechny změny měly být při implementaci oznámeny příslušnému úřadu.

GM2 IS.I.OR.255 Změny systému řízení bezpečnosti informací

VZTAH MEZI ZMĚNAMI ISMS A SOUSTAVNÝM ZLEPŠOVÁNÍM

Změny vyplývající z procesu neustálého zlepšování stanoveného organizací (viz IS.I.OR.260) by měly být řešeny jako jakákoli jiná změna podle pokynů v AMC1 IS.I.OR.255 a GM1 IS.I.OR.255.

PŘÍKLAD ZMĚN, KTERÉ MOHOU MÍT DOPAD NA ISMS

Níže jsou uvedeny některé příklady změn, které mohou mít dopad na ISMS nebo které by mohly vést k nepřijatelné úrovni rizika, a proto by měly podléhat kontrole ze strany příslušného úřadu podle ustanovení stanovených v IS.I.OR.255:

(a) Změny rozsahu ISMS, rozhraní nebo souvisejících politik:

— Organizace rozšiřuje působnosti svého podnikání a integruje další společnost do své organizační struktury.

— Organizace identifikovala neshody naznačující nesprávný rozsah.

— Organizace mění svou politiku a/nebo cíle v oblasti bezpečnosti informací s potenciálním dopadem na bezpečnost letectví.

— Změny rozhraní organizace vyplývající např. ze změn v insourcovaných nebo outsourcovaných činnostech.

(b) Změny v zodpovědnostech a odpovědnosti, jakož i v organizační struktuře zahrnující implementaci a průběžné sledování souladu s tímto nařízením:

— Odpovědný vedoucí delegoval určité povinnosti podle Části IS na osobu nebo skupinu osob.

— Organizace uzavírá smlouvy na činnosti týkající se řízení bezpečnosti informací podle IS.I.OR.235.

(c) Změny používané metodiky řízení rizik:

— Organizace mění klasifikaci pravděpodobnosti nebo dopadů ve své metodice řízení rizik, např. s cílem získat vyšší rozčlenění.

— Organizace implementuje změny ve své metodice řešení rizik.

— Organizace integruje své řízení rizik v oblasti bezpečnosti informací do stávajících systémů řízení.

(d) Změny v procesu správy událostí v oblasti bezpečnosti (security):

— Organizace se rozhodne smluvně zajišťovat činnosti týkající se správy událostí v oblasti bezpečnosti (security).

— Organizace mění proces oznamování událostí v oblasti bezpečnosti (security) a kritéria tak, aby eskalovala k vyššímu vedení pro rychlejší řešení.

— Organizace mění svou politiku pro zmírňování zranitelností.

— Organizace mění svůj postup pro zotavení se (obnovu) z incidentu.

PŘÍKLAD ZMĚN, KTERÉ NEMAJÍ DOPAD NA ISMS

Ne všechny provozní změny související s bezpečností informací mají dopad na ISMS, a proto se ne všechny změny musí hlásit příslušnému úřadu v souladu s ustanoveními uvedenými v IS.I.OR.255. Takovéto změny mohou reprezentovat následující scénáře:

— Po úspěšně detekované události v oblasti bezpečnosti (security), která se mohla snadno vyvinout v incident, se organizace rozhodne spustit rozsáhlou kampaň na zvýšení povědomí o kybernetické bezpečnosti pro všechny zaměstnance.

— Aktualizace programu školení personálu a/nebo obsahu školení jako výsledek procesů neustálého zlepšování zavedených v organizaci.

— Organizace nahrazuje softwarový nástroj, který používá pro šifrování citlivých souborů, jiným softwarovým řešením.

— Organizace se rozhodla provést vnitřní restrukturalizaci z obchodních důvodů, změnit názvy oddělení nebo sekcí, aniž by provedla jakékoli změny v zodpovědnostech a odpovědnosti (např. odpovědný vedoucí) zahrnující ISMS organizace.

— Organizace se rozhodne aktualizovat stávající preventivní kontrolu, např. konfiguraci nového firewallu ve své vnitřní síti.

AMC1 IS.I.OR.260 Soustavné zlepšování

Proces neustálého zlepšování (CIP), jak vyžaduje IS.I.OR.200(b), by se měl zaměřit na soustavné zlepšování účelnosti, vhodnosti a přiměřenosti ISMS. Toho by mělo být dosaženo proaktivním a systematickým posuzováním ISMS a všech jeho prvků – včetně jeho vyspělosti. Posuzování by mělo zohlednit výsledky a závěry dalších procesů bezpečnosti a zajištění informací, včetně auditů, přezkoumání vedením, hodnocení výkonnosti, účelnosti a vyspělosti, jakož i výsledky odvozených nápravných opatření a náprav.

Kroky, které je třeba provést, by měly být alespoň následující:

(a) Identifikace příležitostí ke zlepšení na základě výsledků posouzení ISMS s ohledem na jeho vhodnost, účelnost, přiměřenost, a je-li to považováno za nutné, i efektivnost, jakož i na jakýkoli jiný návrh na zlepšení. Posouzení by mělo vzít v úvahu ukazatele výkonnosti, které odrážejí jeho procesy a prvky a definované cíle účelnosti a vyspělosti.

(b) Vyhodnocení identifikovaných příležitostí z hlediska nákladů a přínosů, absence nebo snížení nežádoucích účinků a dosažení plánovaných cílů a zamýšlených výsledků.

(c) Návrh vyhodnocených možností zlepšení vedení a doporučení činností k podpoře jejich přezkoumání a rozhodování.

(d) Podle rozhodnutí přijatého podle bodu (c) výše – plánování, vývoj a implementace činností a změn ISMS, jeho procesů nebo prvků k dosažení zlepšení.

(e) Vyhodnocení účelnosti realizovaných opatření a změn ISMS a případně ověření, že byla odstraněna kořenová příčina zjištěných nedostatků.

Vedení by mělo v plánovaných intervalech posuzovat a přezkoumávat výsledky CIP, aby zajistilo trvalou účelnost, přiměřenost a vhodnost ISMS, rozhodlo o prioritách provádění činností a změn, jakož i revidovalo nebo stanovilo nové cíle, nebo cíle pro neustálé zlepšování.

GM1 IS.I.OR.260 Soustavné zlepšování

Bod IS.I.OR.260 pokrývá procesy zajištění pro ISMS způsobem, který lze považovat za rovnocenný zajištění bezpečnosti v dokumentu ICAO Doc 9859 „*Safety Management Manual (SMM)*“, který zahrnuje sledování a měření výkonnosti, řízení změn a neustálé zlepšování SMS.

V tomto nařízení:

— IS.I.OR.260(a) se za použití přiměřených ukazatelů výkonnosti zabývá posuzováním účelnosti a vyspělosti ISMS;

— IS.I.OR.260(b) řeší opatření ke zlepšení, tj. nápravy a nápravná opatření, pro nedostatky zjištěné v IS.I.OR.260(a) a proces neustálého zlepšování.

Podobná ustanovení pro neustálé zlepšování jsou obsažena v jiných systémech řízení informací, jako je ISO/IEC 27001 (viz Dodatek II k tomuto dokumentu).

Kontext a prostředí rizik organizací nejsou nikdy statické, a proto vyžadují dynamické přizpůsobení, vývoj a změnu cílů, architektur, organizačních struktur a procesů dané organizace, aby byla rizika bezpečnosti informací udržována na přijatelné úrovni. V důsledku toho by měl být ISMS považován za vyvíjející se a učící se část/prvek organizace, který je třeba neustále monitorovat a zlepšovat, s cílem zajistit sladění s bezpečnostními cíli organizace a účelnost.

CIP si klade za cíl neustále zlepšovat účelnost, vhodnost, přiměřenost a v případě potřeby i effektivnost ISMS. Organizace může začlenit CIP podle Části IS do některých jiných již působících CIP a může použít metody, jako je cyklus plánuj-dělej-kontroluj-jednej (PDCA) *(Plan-Do-Check-Act)* nebo cyklus definuj-měř-analyzuj-vylepši-kontroluj (DMAIC) *(Define-Measure-Analyse-Improve-Control)* (viz také GM1 IS.I.OR.200).

CIP je založen na proaktivním a systematickém posuzování ISMS a všech jeho prvků včetně procesů a kontrol bezpečnosti informací řízených ISMS. Posouzení by mělo být provedeno podle organizačních cílů pro požadované úrovně výkonu, účelnosti a vyspělosti. Tyto cíle, kromě zajištění dosažení vyhovění požadavkům podle tohoto nařízení, mohou také zahrnovat cíle stanovené politikou nebo normami dané organizace a rozhodnutími vedení.

Výše uvedené posouzení je založeno na výsledcích hodnocení výkonnosti, auditů, rizikových a incidentních procesů, jakož i již aplikovaných nápravných opatření a náprav. Některé faktory, které je třeba vzít v úvahu při provádění posouzení, jsou následující:

— **Přiměřenost** se týká toho, zda systém zavádí disciplíny potřebné pro řízení bezpečnosti informací, např. používáním široce uznávaných průmyslových norem, dostatečným způsobem s ohledem na vyhovění požadavkům tohoto nařízení.

— **Účelnost ISMS** a efektivní implementace procesů a kontrol řízených ISMS se posuzuje analýzou, zda:

  — rizika v oblasti bezpečnosti informací jsou řízena tak, aby bylo dosaženo bezpečnostních cílů;

  — bylo dosaženo zamýšlených výsledků ISMS a byly splněny požadavky nebo cíle;

  — všechny typy nedostatků, včetně poruch, jsou řízeny tak, aby splnily nebo správně implementovaly požadavek nebo kontrolu.

— **Efektivita** ISMS se týká implementace zjednodušených procesů; zlepšení efektivity by však neměla mít nepříznivý dopad na účelnost.

Identifikace příležitostí ke zlepšení

Příležitosti ke zlepšení mohou být identifikovány z výsledků posuzování CIP nebo mohou být předloženy jako návrhy z jiných zdrojů. Identifikace často zahrnuje odchylky nebo nápravná opatření, stejně jako neefektivní procesy nebo kontroly, které nejsou napraveny.

Návrhy na zlepšení pocházejí ze zdrojů, jako jsou:

— Řízení rizik: primárním faktorem zlepšování ISMS jsou výsledky pravidelných analýz rizik a následných řešení rizik, kdy proces řešení rizik zahrnuje sledování implementovaných bezpečnostních opatření a vyhodnocování jejich účelnosti.

— Hodnocení výkonnosti a účelnosti: závěry z (klíčových) ukazatelů výkonnosti, jejich měření, analýza a průběžné monitorování a také výsledek posouzení účelnosti včetně výsledků následně aplikovaných náprav a nápravných opatření.

— Hodnocení vyspělosti včetně výsledků následných náprav a nápravných opatření.

— Ponaučení získaná z procesu detekce, zpracování a reakce na incidenty v oblasti bezpečnosti informací a potenciální řešení kořenové příčiny.

— Výsledky (interních) auditů lze použít k ověření, zda ISMS a kontroly v rámci rozsahu auditu splňují požadavky dané organizace, a ke zjištění, kde existují potenciální oblasti pro zlepšení.

— Přezkoumání a vyhodnocení ze strany vedení současného akčního plánu, stanovení nebo revize cílů nebo rozhodnutí o příležitostech a opatřeních ke zlepšení.

— Program návrhů organizace (návrhy na zlepšení), přezkoumání, průzkumy nebo hodnocení se zaměstnanci nebo zpětná vazba od dodavatelů nebo styčných stran.

Jakýkoli výsledek tohoto procesu by měl být zdokumentován. Výsledná opatření mohou být začleněna do zastřešujícího akčního plánu, který je centrálně konsolidován a pravidelně přezkoumáván podle příslušných politik. Výsledný akční plán lze dále rozdělit na taktický, krátkodobý/střednědobý akční plán a strategický, dlouhodobý akční plán.

AMC1 IS.I.OR.260(a) Soustavné zlepšování

(a) **POSOUZENÍ ÚČELNOSTI ISMS**

Při plnění požadavků IS.I.OR.260(a) by organizace měla mít zaveden proces monitorování, měření, hodnocení a přezkoumání účelnosti svého ISMS, který definuje:

(1) kdo monitoruje, měří, analyzuje a vyhodnocuje výsledky a přijímá odpovědná rozhodnutí;

(2) kdy by měly být provedeny výše uvedené kroky;

(3) jaké metody monitorování, měření, analýzy a hodnocení se používají k zajištění srovnatelných a reprodukovatelných výsledků.

Kalendářní základ posuzování by měl být úměrný maximální úrovni rizika stanovené v IS.I.OR.205.

Proces monitorování, měření, hodnocení a přezkoumávání účelnosti ISMS organizace uvedený v AMC1 IS.I.OR.260(a) by měl zahrnovat minimálně:

(1) shromažďování a uchovávání metrik činností a dalších informací, které by mohly být užitečné pro účely monitorování;

(2) analýzu metrik za účelem identifikace trendů a odchylek od předem definovaných výkonnostních cílů.

(b) **POSOUZENÍ VYSPĚLOSTI ISMS**

Organizace by měla posoudit vyspělost svého ISMS pomocí vhodného modelu vyspělosti, aby identifikoval oblasti pro zlepšení ISMS. K tomu by měla organizace:

(1) definovat nebo přijmout model vyspělosti, který představuje soubor důležitých a relevantních procesů a schopností, jejichž implementace a udržování se očekává;

(2) pro každý posuzovaný proces nebo schopnost zajistit, aby model definoval kritéria, podle kterých by měly být při určování úrovně vyspělosti posuzovány a hodnoceny specifické aspekty, charakteristiky a účelnost;

(3) definovat pro každý posuzovaný proces nebo schopnost jejich požadovanou cílovou úroveň vyspělosti.

(c) Pro každý posuzovaný proces nebo schopnost v oblasti bezpečnosti informací obsažené v modelu vyspělosti by organizace měla:

(1) vyhodnotit a zdůvodnit aktuální úroveň vyspělosti;

(2) identifikovat jakoukoli oblast pro zlepšení, které by měl učinit, aby dosáhl cílové úrovně vyspělosti;

(3) shromažďovat a zaznamenávat důkazy o silných a slabých stránkách implementovaného ISMS a jeho vyhodnocené vyspělosti.

GM1 IS.I.OR.260(a) Soustavné zlepšování

(a) Jako obecné vodítko by prvky ISMS, které by měly být monitorovány, měřeny a hodnoceny, měly být minimálně:

(1) proces posuzování a řešení rizik (včetně rizik na rozhraních s jinými organizacemi);

(2) řízení neshod a nápravných opatření;

(3) řízení incidentů a zranitelností;

(4) řízení způsobilosti (kompetencí) persoálu.

(b) Existující modely vyspělosti pro hodnocení ISMS

Jako obecné vodítko pro definici nebo přijetí modelu vyspělosti *(maturity model)*(MM) lze zvážit následující existující modely:

— *Cybersecurity Capability Maturity Model* (C2M2), verze 1.1: tento model byl zveřejněn Ministerstvem energetiky USA v roce 2014. Zavádí pojem úrovně indikátoru splatnosti − *Maturity Indicator Levels* (MIL) v rozsahu od 0 do 3 a zabývá se nejen úrovněmi výkonnosti, ale také postupy provedení (v rámci cílů přístupu a progrese přístupu) a také postupy zajištění (v rámci cílů řízení a progrese institucionalizace).

— *Systems Security Engineering – Capability Maturity Model* (SSE-CMM): zveřejněn organizací ISO jako ISO 21827 v roce 2008. Zaměřuje se na inženýrské postupy, mnohem méně na provozní postupy, které jsou rozděleny do 11 „základních bezpečnostních postupů − *Security Base Practices*“ a 11 „základních projektových a organizačních postupů − *Project and Organizational Base Practices*“. Zavádí pojem pěti úrovní schopností, od „neformálně prováděné − *Performed Informally*“ po „neustále se zlepšující − *Continuously Improving*“.

— *NIST Cybersecurity Framework* (NIST CSF), verze 1.1: zveřejněn institutem NIST v dubnu 2018. Ačkoli není navržen jako MM, rámec definuje čtyři „implementační úrovně − *Implementation Tiers*“, od „částečné − *Partial*“ po „adaptivní − *Adaptive*“, které jsou kvalitativním měřítkem organizačních postupů řízení rizik kybernetické bezpečnosti. Zaměřuje se na funkčnost a opakovatelnost řízení rizik kybernetické bezpečnosti.

— *ATM Cybersecurity Maturity Model*, edice 1: publikován v únoru 2019 EUROCONTROL NM pro organizace v oblasti ATM. I když není navržen pro širší použití, lze jej podle potřeby upravit. Definuje pět úrovní vyspělosti, od „neexistující − *Non-existent*“ po „adaptivní − *Adaptive*“, inspirované terminologií „Tier“ z NIST CSF. Ve skutečnosti je model založen na NIST CSF spolu s některými prvky ISO/IEC 27001.

Následující Tabulka 1 mapuje výše uvedené MM na hypotetický pětiúrovňový MM.

Tabulka 1: Matice mapování existujícího MM na hypotetický pětiúrovňový MM

Mapování na pětiúrovňový MM	C2M2	Eurocontrol NM	ISO 21827	NIST CSF 1.1
Initial (počáteční)	MIL 0	Non-Existent	Performed Informally	
Defined (definovaná)	MIL 1 (Initial)	Partial	Planned & Tracked	Partail
Implemented (implementovaná)	MIL 2 (Identified)	Defined	Well defined	Risk-Informed
Managed (řízená)	MIL 3 (Managed)	Assured	Quantitatively Controlled	Repeatable
Improved (zlepšená)		Adaptive	Continuously Improving	Adaptive

Není vyžadována žádná konkrétní úroveň vyspělosti. Pokud však bude dosaženo souladu, organizace určí, které požadavky kterých modelů již byly splněny (povinné), a mohou se rozhodnout dosáhnout úrovně, která je pro danou organizaci výhodná (dobrovolné). V dlouhodobějším horizontu může dosažení vyšších úrovní vyspělosti zvýšit důvěru úřadů dozoru, což může mít dopad na úroveň činností dozoru týkajících se takovéto organizace.

AMC1 IS.I.OR.260(b) Soustavné zlepšování

Pokud je zjištěn nedostatek, měla by organizace včas reagovat podle definovaného procesu vedoucího ke zvládnutému (řízenému) stavu, pokud jde o nedostatek, jeho související důsledky a v případě potřeby prevenci jeho budoucího opakování nebo výskytu jinde.

Na základě vyhodnocení dopadu a rozsahu nedostatku a potenciálních důsledků na ISMS by měl proces zahrnovat jako kritéria pro vyhovění:

(a) rozhodování o nápravách a jejich provedení bez zbytečného odkladu za účelem omezení dopadu nedostatku a řešení jeho důsledků a případně jeho kontroly nebo odstranění;

(b) rozhodování o potřebě a provedení nápravných opatření k odstranění příčiny a faktorů přispívajících k nedostatku na základě analýzy kořenové příčiny a vyhodnocení opatření k nápravě příčiny s cílem být úměrné následkům a dopadu nedostatku;

(c) ověřování provedených činností:

(1) aby byly účinné a vedly k přijatelným zbytkovým rizikům;

(2) aby neměly nezamýšlené vedlejší účinky vedoucí k dalším nedostatkům, novým rizikům nebo ISMS, který není v souladu s platnými požadavky; jakož i

(3) aby se v případě nápravných opatření účinně napravila nebo odstranila kořenová příčina;

(d) hlášení a přezkoumávání zjištěných nedostatků, akčního plánu a výsledků opatření přijatých odpovědným vedoucím organizace nebo delegovanou osobou (osobami) a v případě potřeby s dalšími zúčastněnými nebo dotčenými rolemi a stranami;

(e) dokumentování jako důkazu zjištěných nedostatků, plánovaných a realizovaných náprav a/nebo nápravných opatření spolu s termíny a odpovědnými osobami, zpětné vazby vedení, výsledků procesního kroku podle bodu (c) výše a v případě potřeby rozhodnutí o změně přijaté pro samotný ISMS.

GM1 IS.I.OR.260(b) Soustavné zlepšování

„Nezbytná opatření ke zlepšení“ uvedená v IS.I.OR.260(b) se týkají náprav nebo nápravných opatření k odstranění nedostatků nebo opatření zaměřených na zlepšení účelnosti a vyspělosti ISMS.

Proces splňující kritéria definovaná v AMC1 IS.I.OR.260 by měl zahrnovat následující aspekty:

(a) identifikování rozsahu, dopadu, kontextu a spouštěčů nedostatku, jeho vyhodnocení podle některých stanovených kritérií, analyzování potenciálních důsledků pro ISMS včetně potenciální existence v jiných oblastech;

(b) rozhodování o nápravách a jejich provádění k okamžitému omezení dopadu a zvládání (řízení) následků nedostatku a případně k jeho kontrole nebo odstranění;

(c) rozhodování o nápravných opatřeních nezbytných k odstranění (kořenové) příčiny (příčin) nedostatku, která jsou úměrná následkům;

(d) opětovné posuzování prvků ISMS, které mohou být ovlivněny realizovanými opatřeními, aby se zajistilo, že nevznikne žádné další riziko;

(e) ověřování provedených činností uvedených v bodě (c) AMC1 IS.I.OR.260(b);

(f) hlášení a přezkoumávání výsledků kroků procesu s vedením (viz bod (d) AMC1 IS.I.OR.260(b));

(g) dokumentování a dokládání výsledku výše uvedených procesních kroků (viz bod (e) AMC1 IS.I.OR.260(b)).

Dodatek I
Příklady scénářů hrozeb s potenciálním škodlivým dopadem na bezpečnost

Níže je uveden nevyčerpávající seznam příkladů scénářů hrozeb v oblasti bezpečnosti informací s potenciálním škodlivým dopadem na bezpečnost, které mohou úřady a organizace zvážit.

Příklad 1: Digitální spojení letadlo – ATC

— **Aktiva/doména vektoru hrozby**

  — hlasové a pozemní automatizované systémy ATC

  — poskytovatelé pozemních komunikací

  — poskytovatelé služeb VF spojení letadlo – země / země – letadlo

  — letadla a prostředky používané pro hlasové spojení a komunikaci datovým spojem

— **Nevyčerpávající souhrn potenciálních hrozeb**

  — hrozba (dostupnost): překročení výkonnosti systému, saturace komunikačního kanálu

  — hrozba (integrita): MITM útoky *(man-in-the-middle attack)* nebo útoky typu injekce *(injection attack)*

  — hrozba (důvěrnost): pasivní naslouchání komunikaci, špehování hardwarových zařízení

— **Souhrn scénářů hrozeb a jejich potenciálních škodlivých dopadů na bezpečnost**

  — Narušení služeb brání spojení ATC s jedním nebo více letadly a/nebo pozemním systémem ATC.

  — Manipulace s daty prostřednictvím MITM útoku by pilotovi a/nebo systému ATC poskytla nepravdivé informace, což může vytvořit bezpečnostní riziko, nebo vložení dat do letadla nebo pozemních systémů s cílem narušit službu a schopnosti.

  — Neexistují žádné specifické regulační požadavky na šifrování dat nebo hlasu pro komunikaci datovým spojem; z důvodu zachování důvěrnosti by však zařízení používaná k poskytování a dodávkám služeb měla být kontrolována a omezena pouze na ty zdroje, které vyžadují přístup, aby bylo zajištěno, že služby nemohou být jakýmkoli způsobem narušeny a manipulovány.

Příklad 2: Nedovolená manipulace s daty letového provozu

— **Aktiva/doména vektoru hrozby**

  — poskytovatel internetových služeb (ISP)

  — síť (sítě) služeb ATM

  — přehledová data

  — systémy ATC

— **Nevyčerpávající souhrn potenciálních hrozeb**

  — Kompromitace ISP (confidentiality): Útočník získá neoprávněný přístup k systémům nebo infrastruktuře ISP poskytujícího služby sítě systému ATM.

  — Manipulace s daty (integrita): Jakmile je ISP kompromitován, útočník by mohl manipulovat s daty při přenosu. To by mohlo zahrnovat vložení (injekce) falešných dat nebo odstranění/úpravu dat legitimních.

  — Odmítnutí služby (dostupnost): Útočník by také mohl potenciálně zcela narušit datovou komunikaci, což by mělo za následek odmítnutí služby (DoS) systému.

— Injekce malwaru (integrita/dostupnost): Útočník by mohl potenciálně využít kompromitovaného ISP jako odrazový můstek k vložení malwaru do systémů, což by způsobilo další narušení nebo umožnilo další útoky.

— **Souhrn scénářů hrozeb a jejich potenciálních škodlivých dopadů na bezpečnost**

— Kompromitace ISP: Zachycení citlivých dat a/nebo manipulace s nimi mající dopad na bezpečné řízení letového provozu.

— Manipulace s daty: Nesprávné situační povědomí, které může mít za následek snížení rozstupů mezi letadly a nesprávná rozhodnutí řízení letového provozu.

— Odmítnutí služby: Snížení schopnosti ATC zajišťovat rozstup vedoucí k aktivaci postupů pro nenadálé události, včetně snížení kapacity, s případnou možností uzavření velkých oblastí vzdušného prostoru.

Příklad 3: Dodavatelský řetězec softwaru a pozemní infrastruktura provozovatele letadla, CAMO a organizací k údržbě letadel, včetně vybavení používaného k podpoře řízení, provozu a údržby letadel

— **Aktiva/doména vektoru hrozby**

— dodavatelský řetězec provozovatelů letadel, CAMO a organizací k údržbě

— interní pozemní infrastruktura provozovatele letadla nebo údržby používaná ke správě letadel a provozu (hardware/software) a další aktiva informačních technologií

— aktiva informačních technologií používaná k aktualizaci systémů v letadle (software a hardware) používaných pro činnosti údržby

— **Nevyčerpávající souhrn potenciálních hrozeb**

— hrozba (dostupnost): narušení hardwaru/softwaru/systému

— hrozba (integrita): kompromitovaný hardware/software/systém

— hrozba (důvěrnost): kompromitovaný hardware/software/systém

— **Souhrn scénářů hrozeb a jejich potenciálních škodlivých dopadů na bezpečnost**

— Narušení šíření meteorologických informací, když je letadlo ve vzduchu, může snížit schopnost letové posádky vyhnout se potenciálně nebezpečným meteorologickým podmínkám (např. silným bouřím/mlze v noci).

— Manipulace s navigačními daty/navigační databází bude mít za následek, že letovým plánům a zobrazením navigačních informací nelze věřit.

— Nedostatek kontroly a přístupu k informacím, jako je program údržby flotily nebo plánování letových posádek, ovlivňuje schopnost organizací udržovat bezpečný provoz.

Použití motýlkové analýzy na tento příklad

Kombinují se dvě koordinované motýlkové analýzy různých dimenzí rizik, protože konečný zájem spočívá pouze v důsledcích pro bezpečnost letectví.

Prvek motýlkové analýzy informační bezpečnosti (security)	Prvek motýlkové analýzy bezpečnosti (safety) letectví
Hrozby informační bezpečnosti 1) zneužití zranitelnosti hardwaru/softwaru: narušená funkce systému 2) zneužití zranitelnosti hardwaru/softwaru: kompromitována integrita systému	

Prvek motýlkové analýzy informační bezpečnosti (security)	Prvek motýlkové analýzy bezpečnosti (safety) letectví
3) zneužití zranitelnosti hardwaru/softwaru: kompromitována důvěrnost informací zpracovávaných systémem (systémy)	
Preventivní bariéry informační bezpečnosti	
Nebezpečí & hlavní události informační bezpečnosti 1) narušená funkčnost systému (nebezpečí) → narušená/nespolehlivá funkčnost systému 2) kompromitovaná integrita systému (nebezpečí) → funkce systému nepředvídatelná 3) informace odhalitelné (nebezpečí) → nezjistitelná exfiltrace informací	Hrozby pro bezpečnost 1) narušená/nespolehlivá funkčnost systému 2) funkce systému nepředvídatelná 3) nezjistitelná exfiltrace informací
Zmírňující bariéry informační bezpečnosti	Preventivní bariéry pro bezpečnost 1) použití kontroly přístupu u správy systému 2) atd.
Následky pro informační bezpečnost 1) ztráta funkce systému (= výpadek výrobního systému) 2) ztráta integrity funkce systému (= některá funkce systému chybná/nefunkční) 3) ztráta důvěrnosti informací (= některé informace mohou uniknout)	Nebezpečí & hlavní události pro bezpečnost: 1) ztráta funkce systému (nebezpečí) → *v provozním systému údržby* 2) ztráta integrity funkce systému (nebezpečí) → *systémy pracují s nesprávnými informacemi* 3) ztráta důvěrnosti informací (nebezpečí) → *únik důvěrných informací o údržbě a vnitřku letadla*
	Zmírňující bariéry pro bezpečnost 1) použití záložních postupů, aby se zabránilo chybným úkonům údržby 2) použití postupů k zabezpečení integrity softwaru letadla
	Následky pro bezpečnost 1) chybné úkony údržby 2) nesprávně provedené úkony údržby 3) exfiltrace informací umožňuje identifikaci zranitelností 4) narušení systémů letadla, nepředvídatelná funkce systému, ztráta významných systémů letadla (jako je ovládání motoru)

Příklad 4: Software projekčních a výrobních organizací, dodavatelský řetězec, konstrukční a výrobní pozemní infrastruktura

— **Aktiva/doména vektoru hrozby**

  — dodavatelský řetězec částí, hardwaru a softwaru projekčních a výrobních organizací

  — interní pozemní infrastruktura projekčních a výrobních organizací používaná ke správě softwaru/hardwaru používaných při výrobě a vývoji produktů, které budou používat výrobci letadel, provozovaté nebo prostředky informačních technologií pozemních automatizačních systémů ATM/ANS (hardware/software).

— aktiva informačních technologií projekčních a výrobních organizací používaná jejich zákazníky k aktualizaci systémů v letadle (softwaru/hardwaru) používaných pro úkony údržby nebo pozemních automatizačních systémů ATM/ANS.

— **Nevyčerpávající souhrn potenciálních hrozeb**

— hrozba (dostupnost): systémy používané k ukládání, přenosu a výměně informací jsou kvůli útokům DoS pro zásadní úkony nedostupné

— hrozba (integrita): systémy používané k ukládání, přenosu a výměně informací jsou prostřednictvím MITM útoků kompromitovány

— hrozba (důvěrnost): k systémům používaným k ukládání, přenosu a výměně informací mají přístup vnitřní nebo vnější hrozby

— **Souhrn scénářů hrozeb a jejich potenciálních škodlivých dopadů na bezpečnost**

— Narušení systémů používaných k ukládání, přenosu a výměně informací způsobem, který by bránil řádnému řízení letadla a jeho systémů a nepříznivě ovlivnil provoz letadla.

— Systémy používané k ukládání, přenosu a výměně informací již nelze považovat za důvěryhodné. Pokud nejsou udržovány na takové úrovni, aby bylo zajištěno, že veškerou výměnu informací, data a software lze považovat za důvěryhodné, dojde k přerušení pozemního provozu i provozu letadel.

— Díky nekontrolovanému přístupu k systémům používaným k ukládání, přenosu a výměně informací (včetně informací, které jsou přijímány a vyměňovány s dodavatelským řetězcem) mohou být opatřeny technické detaily, které by mohly být použity k vytvoření sofistikovanějších útoků zaměřených na systémy kritické z hlediska bezpečnosti.

Příklad 5: Systém výcviku

— **Aktiva/doména vektoru hrozby**

— dodavatelský řetězec veškerého softwaru a hardwaru, který bude použit v systémech výcviku nebo výcvikových zařízeních (včetně letových simulátorů) používaných k výcviku pilotů nebo personálu pozemních systémů ATM/ANS

— interní infrastruktura použitá ve veškerém softwaru a hardwaru, který bude použit při návrhu, výrobě nebo produkci produktů (hardwaru nebo softwaru), které budou použity v letadlech nebo pozemních systémech ATM/ANS

— správa interních operačních domén a systému veškerého softwaru a hardwaru, který bude použit při návrhu, výrobě nebo produkci produktů (hardwaru nebo softwaru), které budou použity v letadlech nebo pozemních systémech ATM/ANS

— **Nevyčerpávající souhrn potenciálních hrozeb**

— hrozba (dostupnost): systémy výcviku nebo výcviková zařízení jsou pomocí útoků DoS znepřístupněny, když je potřeba je použít

— hrozba (integrita): systémy výcviku nebo výcviková zařízení jsou prostřednictvím MITM útoků kompromitovány

— hrozba (důvěrnost): k funkčním modelům, informacím a datům, které jsou zabudovány do systémů výcviku nebo výcvikových zařízení, mají přístup vnitřní nebo vnější hrozby

— **Souhrn scénářů hrozeb a jejich potenciálních škodlivých dopadů na bezpečnost**

— Narušení systémů výcviku (hardwaru a softwaru) bude mít dopad na schopnost organizací udržet si kvalifikovaný personál. Rovněž by to zabránilo letadlu a jeho systémům ve správném provozu a ovlivnilo by úkony údržby pozemních systémů ATM/ANS.

— Model výcviku nebo způsoby poruch a související nouzové podmínky se liší od skutečného chování leteckého systému, a proto vyvolávají nepřiměřené reakce. Pokud systémům výcviku nelze důvěřovat, ovlivní to schopnost organizací udržovat dostatečně kvalifikovaný personál pro svůj provoz (piloti, personál údržby nebo pozemní personál ATM/ANS, který prošel nesprávným výcvikem, by měl být rekvalifikován).

— Nedostatek kontroly a přístupu k systémům výcviku ovlivňuje schopnost organizací udržovat systém výcviku, o kterém je známo, že je v důvěryhodném stavu. Navíc nekontrolovaný přístup k systémům výcviku, které obsahují funkční modely, informace a data, může poskytnout technické detaily, které by mohly být použity k vytvoření sofistikovanějších útoků na samotný systém výcviku nebo na systém kritický z hlediska bezpečnosti v reálném světě.

Příklad 6: Letištní systém dodávky paliva a související infrastruktura

— **Aktiva/doména vektoru hrozby**

— pozemní infrastruktura skladování a distribuce paliva

— digitální systémy používané k řízení čerpání a měření množství paliva

— dodavatelský řetězec pro dodávky paliva, včetně dodavatelů paliva třetích stran

— aktiva letištní informační technologie používaná pro řízení zásob paliva a plánování dodávek

— **Nevyčerpávající souhrn potenciálních hrozeb**

— hrozba (dostupnost): přerušení plnění palivem nebo systémů dodávek paliva

— hrozba (integrita): manipulace s palivovými řídicími systémy nebo měřicími zařízeními

— hrozba (důvěrnost): neoprávněný přístup k údajům o plnění palivem a dodávkách paliva

— **Souhrn scénářů hrozeb a jejich potenciálních škodlivých dopadů na bezpečnost**

— Přerušení dodávky paliva může vést ke zpoždění nebo zrušení letů, což může způsobit provozní výpadky a potenciální bezpečnostní problémy, pokud se zásoby paliva kriticky sníží.

— Manipulace se systémy řízení paliva nebo měřicími zařízeními by mohla vést k plnění nesprávného množství paliva do letadla, což by ovlivnilo výpočty hmotnosti a vyvážení letadla a mohlo by způsobit incidenty související s vyčerpáním paliva.

— Neoprávněný přístup k údajům o plnění paliva by mohl umožnit aktérům hrozby manipulovat s údaji o plánování nebo zásobách paliva, což by mohlo způsobit narušení provozu letiště a dostupnosti paliva pro letadla.

Příklad 7: Systém NOTAM příslušného vnitrostátního úřadu a související infrastruktura

— **Aktiva/doména vektoru hrozby**

— infrakstruktura a digitální rozhraní vnitrostátního systému NOTAM

— dodavatelský řetězec pro údržbu a aktualizace systému NOTAM

— IT aktiva příslušného vnitrostátního úřadu používaná pro vytváření, distribuci a uložení NOTAM

— **Nevyčerpávající souhrn potenciálních hrozeb**

— hrozba (dostupnost): narušení systému NOTAM nebo jeho přístupu

— hrozba (integrita): manipulace s daty NOTAM nebo neoprávněné vytvoření NOTAM

— hrozba (důvěrnost): neoprávněný přístup k datům NOTAM

— **Souhrn scénářů hrozeb a jejich potenciálních škodlivých dopadů na bezpečnost**

  — Narušení systému NOTAM by mohlo zabránit šíření kritických leteckých informací pilotům a řídícím letového provozu, potenciálně vedoucímu k bezpečnostním problémům.

  — Manipulace s daty NOTAM nebo neoprávněné vytváření zpráv NOTAM by mohlo vést k šíření nesprávných informací, což může vést k tomu, že piloti činí rozhodnutí na základě nepravdivých nebo zavádějících údajů.

  — Neoprávněný přístup k datům NOTAM by mohl vést k úniku informac,í potenciálně odhalujícímu citlivé provozní informace.

Příklad 8: Systém příkazů k zachování letové způsobilosti (AD) leteckého úřadu a související infrastruktura

— **Aktiva/doména vektoru hrozby**

  — infrakstruktura a digitální rozhraní systému EASA AD

  — dodavatelský řetězec pro údržbu a aktualizace systému AD

  — IT aktiva EASA používaná pro vytváření, distribuci a uložení AD

— **Nevyčerpávající souhrn potenciálních hrozeb**

  — hrozba (dostupnost): narušení systému AD nebo jeho přístupu

  — hrozba (integrita): manipulace s daty AD nebo neoprávněné vytvoření AD

  — hrozba (důvěrnost): neoprávněný přístup k datům AD

— **Souhrn hrozeb a jejich potenciálních škodlivých dopadů na bezpečnost**

  — Narušení systému AD by mohlo zabránit šíření kritických informací pro letovou způbilost provozovatelům letadel a organizacím pro údržbu, potenciálně vedoucímu k bezpečnostním problémům.

  — Manipulace s daty AD nebo neoprávněné vytváření AD by mohlo vést k šíření nesprávných informací, což by mohlo vést k tomu, že provozovatelé letadel a organizace pro údržbu se rozhodují na základě nepravdivých nebo zavádějících údajů.

  — Neoprávněný přístup k datům AD by mohl vést k úniku informací, potenciálně odhalujícímu citlivé provozní informace.

Dodatek II
Hlavní úkoly vyplývající z implementace Části IS, včetně mapy vztahů kompetencí dle NIST CSF 1.1 a článků a prostředků řízení dle ISO/IEC 27001

Hlavní úkol dle Části IS	Typ činnosti	Reference					
	Řízení, Provozní	Část IS	NIST CSF verze 1.1		ISO/IEC 27001		
			Funkce	Kategorie	Ustanovení odstavce	Annex A Control	
						:2013	:2022
Vytvořit a provozovat systém řízení bezpečnosti informací (ISMS)	Řízení	IS.I.OR.200(a)	IDENTIFIKOVAT	ID.RM	4 6.1.1		
Stanovit rozsah ISMS podle požadavků Části IS	Řízení	IS.I.OR.205(a)	IDENTIFIKOVAT	ID.BE-2 ID.BE-4 ID.AM-5	4.3		
Implementovat a udržovat politiku bezpečnosti informací	Řízení	IS.I.OR.200(a)(1)	IDENTIFIKOVAT	ID.GV-1	5.2	A5.1	A5.1
Identifikovat a přezkoumat rizika bezpečnosti informací	Řízení	IS.I.OR.200(a)(2) IS.I.OR.205	IDENTIFIKOVAT	ID.GV-4 ID.RA	6.1.2 8.1 8.2		
Implementovat opatření pro řešení rizik bezpečnosti informací	Řízení	IS.I.OR.200(a)(3) IS.I.OR.210	CHRÁNIT	PR.PT	6.1.3 8.1 8.3		
Implementovat opatření k detekci událostí informační bezpečnosti a identifikovat ty, které se týkají bezpečnosti letectví	Řízení	IS.I.OR.200(a)(5) IS.I.OR.220	DETEKOVAT	DE.AE-3 DE.CM-1 DE.CM-2 DE.CM-3		A11.1.2 A12.4.1 A12.4.3 A16.1.7	A7.2 A8.15 A5.28
Implementovat opatření, která byla oznámena příslušným úřadem	Provozní	IS.I.OR.200(a)(6)			10.1	A6.1.3	A5.5
Přijmout vhodná nápravná opatření k řešení nálezů oznámených příslušným úřadem (neshod)	Obojí	IS.I.OR.200(a)(7) IS.I.OR.225			10.1	A6.1.3	A5.5

Hlavní úkol dle Části IS	Typ činnosti	Reference					
	Řízení, Provozní	Část IS	NIST CSF verze 1.1		ISO/IEC 27001		
			Funkce	Kategorie	Ustanovení odstavce	Annex A Control	
						:2013	:2022
Implementovat systém externích hlášení v oblasti bezpečnosti informací	Řízení	IS.I.OR.200(a)(8) IS.I.OR.230	REAGOVAT	RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5	7.4	A6.1.3 A16.1.2 A16.1.3	A5.5 A6.8
Sledovat dodržování tohoto nařízení a hlásit nálezy vrcholovému vedení	Provozní	IS.I.OR.200(a)(12)	IDENTIFIKOVAT	ID.GV-3	9.2	A18.2.1 A18.2.2	A5.35 A5.36
Chránit důvěrnost vyměňovaných informací	Provozní	IS.I.OR.200(a)(13)	CHRÁNIT	PR.DS-1 PR.DS-2		A8.2.2 A13.2	A5.13 A5.14
Implementovat a udržovat proces neustálého zlepšování pro měření účelnosti a vyspělosti ISMS a usilovat o jeho zlepšování	Řízení	IS.I.OR.200(b) IS.I.OR.260	IDENTIFIKOVAT	ID.RA-6 ID.SC-4	4.4 9.1 9.3 10.1 10.2	A5.1.2 A16.1.7 A17.1.3 A18.2.1	A5.1 A5.28 A5.29 A5.35
			CHRÁNIT	PR.IP-7 PR.IP-10			
			DETEKOVAT	DE.DP-5			
			REAGOVAT	RS.MI-3 RS.IM-2			
			OBNOVIT	RC.IM-2			
Dokumentovat a udržovat všechny klíčové procesy, postupy, role a odpovědnosti	Řízení	IS.I.OR.200(c)	IDENTIFIKOVAT	ID.AM-6 ID.GV-4 ID.RM-1 ID.SC-1 ID.SC-2	4.2 5.2 5.3	A5.1 A6.1.1	A5.1 A5.2
			CHRÁNIT	PR.AT-2 PR.AT-4 PR.AT-5 PR.IP-12			
			DETEKOVAT	DE.DP-1			
			REAGOVAT	RS.CO-1 RS.AN-5			

Hlavní úkol dle Části IS	Typ činnosti	Reference					
	Řízení, Provozní	Část IS	NIST CSF verze 1.1		ISO/IEC 27001		
			Funkce	Kategorie	Ustanovení odstavce	Annex A Control	
						:2013	:2022
Identifikovat všechny prvky, které by mohly být vystaveny rizikům bezpečnosti informací	Řízení	IS.I.OR.205(a)	IDENTIFIKOVAT	ID.AM-1 ID.AM-2 ID.AM-4 ID.AM-5	4.3	A8.1.1	A5.9
Identifikovat rozhraní s jinými organizacemi, která by mohla vést k vystavení se rizikům bezpečnosti informací	Řízení	IS.I.OR.205(b)	IDENTIFIKOVAT	ID.BE-1 ID.BE-2 ID.BE-4 ID.BE-5	4.3		
Identifikovat rizika bezpečnosti informací a přiřadit úroveň rizika	Řízení	IS.I.OR.205(c)	IDENTIFIKOVAT	ID.RA-1 ID.RA-2 ID.RA-3 ID.RA-4 ID.RA-5	6.1.2		
Přezkoumat a aktualizovat posouzení rizik na základě určitých kritérií	Provozní	IS.I.OR.205(d)	IDENTIFIKOVAT	ID.RM	8.2		A5.7
Organizace podle Hlavy C Přílohy III (Část ATM/ANS.OR) k nařízení (EU) 2017/373 sdílejí posouzení podpory bezpečnosti	Provozní	IS.I.OR.205(e)					
Vypracovat a implementovat opatření k řešení rizik a ověřit jejich účelnosti	Provozní	IS.I.OR.210(a)	CHRÁNIT	PR.IP PR.PT	6.1.3 8.3		
Sdělit výsledek posouzení rizik vedení, ostatnímu personálu a dalším organizacím sdílejícím rozhraní	Provozní	IS.I.OR.210(b)	IDENTIFIKOVAT	ID.AM-3 ID.BE-1 ID.BE-2 ID.BE-4 ID.RM-3 ID.SC-3	8.1		
			CHRÁNIT	PR.IP-7			

Hlavní úkol dle Části IS	Typ činnosti	Reference					
	Řízení, Provozní	Část IS	NIST CSF verze 1.1		ISO/IEC 27001		
			Funkce	Kategorie	Ustanovení odstavce	Annex A Control	
						:2013	:2022
Vytvořit systém interních hlášení v oblasti bezpečnosti informací, který umožní shromažďovat a vyhodnocovat události v oblasti bezpečnosti informací od personálu	Řízení	IS.I.OR.200(a)(4) IS.I.OR.215(a) IS.I.OR.215(e)	IDENTIFIKOVAT	ID.AM-3	7.4	A16.1.1 A16.1.2	A5.28 A6.8
Zajistit, aby smluvní organizace hlásily události v oblasti bezpečnosti informací	Řízení	IS.I.OR.215(c)	REAGOVAT	RS.CO-2 RS.CO-4	7.4	A15.1.1 A16.1.2	A5.19 A6.8
Analyzovat interně hlášené události s cílem identifikovat události, incidenty a zranitelnosti v oblasti bezpečnosti informací	Provozní	IS.I.OR.215(b)(1)–(b)(3)	IDENTIFIKOVAT	ID.RA-1		A12.6.1 A16.1.1 A16.1.4	A8.8 A5.24 A5.25
			DETEKOVAT	DE.AE-2 DE.AE-3 DE.AE-5			
Implementovat opatření k detekci událostí v oblasti bezpečosti informací v procesech a provozu, které mohou mít potenciální dopad na bezpečnost letectví	Provozní	IS.I.OR.220(a)	DETEKOVAT	DE.AE DE.CM DE.DP		A11.1.2 A12.4.1 A12.6.1 A16.1.1 A16.1.2 A16.1.3 A16.1.4 A16.1.5	A7.2 A8.8 A8.15 A8.16 A5.24 A5.25 A5.26 A6.8
			CHRÁNIT	PR.PT-1			
Implementovat opatření k reakci na události bezpečnosti informací, které mohou způsobit incident v oblasti bezpečnosti informací	Provozní	IS.I.OR.220(b)	REAGOVAT	RS.RP RS.AN RS.MI		A16.1.5	A5.26

Hlavní úkol dle Části IS	Typ činnosti	Reference					
	Řízení, Provozní	Část IS	NIST CSF verze 1.1		ISO/IEC 27001		
			Funkce	Kategorie	Ustanovení odstavce	Annex A Control	
						:2013	:2022
Spolupracovat na vyšetřování s dalšími organizacemi, které se podílejí na bezpečnosti informací jeho vlastních činností	Řízení	IS.I.OR.215(d)	REAGOVAT	RS.AN-3 RS.AN-5		A15.1.2 A15.1.3 A16.1.7	A5.20 A5.21 A5.28
Implementovat opatření k zotavení se (obnově) z incidentů v oblasti bezpečnosti informací	Provozní	IS.I.OR.220(c)	OBNOVIT	RC.RP-1 RC.IM-1		A16.1.5 A16.1.6	A5.26 A5.27
Řídit rizika spojená se smluvními činnostmi s ohledem na řízení bezpečnosti informací	Řízení	IS.I.OR.235	IDENTIFIKOVAT	ID.SC-1 ID.SC-2		A15.1 A15.2	A5.19 A5.20 A5.21 A5.22
Vytvořit a udržovat proces, který zajistí, že bude k dispozici dostatek personálu pro provádění všech činností týkajících se řízení bezpečnosti informací	Řízení	IS.I.OR.240(f)	IDENTIFIKOVAT	ID.AM-5 ID.AM-6 ID.GV-2	7.1	A6.1.1	A5.2
Vytvořit a udržovat proces, který zajistí, že personál bude mít nezbytnou způsobilost (kompetenci) pro činnosti týkající se řízení bezpečnosti informací	Řízení	IS.I.OR.240(g)	IDENTIFIKOVAT CHRÁNIT	ID.AM-5 ID.AM-6 PR.AT-1	7.2	A7.2.2	A6.3
Vytvořit a udržovat proces, který zajistí, že personál uznává odpovědnosti	Řízení	IS.I.OR.240(h)	IDENTIFIKOVAT	ID.GV-2 ID.GV-3	7.3 7.4	A7.1.2	A6.2

Hlavní úkol dle Části IS	Typ činnosti	Reference					
	Řízení, Provozní	Část IS	NIST CSF verze 1.1		ISO/IEC 27001		
			Funkce	Kategorie	Ustanovení odstavce	Annex A Control	
						:2013	:2022
spojené s přidělenými rolemi a úkoly							
Ověřovat identitu a důvěryhodnost personálu, který má přístup k informačním systémům	Řízení	IS.I.OR.240(i)	CHRÁNIT	PR.AC-6 PR.IP-11	7.1	A7.1.1	A6.1
Archivovat, chránit a uchovávat záznamy a zajistit, že jsou vysledovatelné po stanovenou dobu	Provozní	IS.I.OR.245	IDENTIFIKOVAT	ID.RA-4	7.5	A8.2.2 A8.2.3 A11.1.3 A11.1.4 A12.1.3 A12.3.1 A12.4.1 A12.4.2 A12.4.3	A5.10 A5.13 A7.3 A7.5 A8.6 A8.10 A8.13 A8.15
			CHRÁNIT	PR.AC-2 PR.AC-3 PR.AC-4 PR.DS-1 PR.DS-4 PR.DS-5 PR.DS-6 PR.IP-4 PR.IP-6 PR.PT-1			
Provést nápravu nálezů neshod na základě oznámení příslušného úřadu ve lhůtě dohodnuté s příslušným úřadem	Provozní	IS.I.OR.225			10.1	A18.1.1 A18.2	A5.31 A5.35 A5.36
Implementovat systém hlášení v oblasti bezpečnosti informací v souladu s nařízením (EU) č. 376/2014	Řízení	IS.I.OR.230(a)					
Hlásit incidenty nebo zranitelnosti bezpečnosti informací příslušnému úřadu a za určitých podmínek i ostatním	Provozní	IS.I.OR.230(b) IS.I.OR.230(c)	DETEKOVAT	DE.DP-3	7.4	A16.1.1 A16.1.2 A16.1.3	A5.24 A6.8
			REAGOVAT	RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5			
			OBNOVIT	RC.CO-3			

Hlavní úkol dle Části IS	Typ činnosti	Reference					
	Řízení, Provozní	Část IS	NIST CSF verze 1.1		ISO/IEC 27001		
			Funkce	Kategorie	Ustanovení odstavce	Annex A Control	
						:2013	:2022
Pravidelně posuzovat účelnost a vyspělost ISMS	Provozní	IS.I.OR.260(a)			9	A5.1.2 A12.7.1 A16.1.6	A5.1 A5.27 A8.34
V případě potřeby podniknout kroky ke zlepšení ISMS. Opětovně posoudit prvky ISMS ovlivněné implementovanými opatřeními.	Provozní	IS.I.OR.260(b)			10	A5.1.2	A5.1
Zajistit příslušnému úřadu přístup ke smluvní organizaci	Řízení	IS.I.OR.235(b)			9.3	A6.1.3 A15.1 A15.2	A5.5 A5.20 A5.22
Vrcholové vedení zajistí, aby byly k dispozici veškeré zdroje nezbytné ke splnění tohoto nařízení	Řízení	IS.I.OR.240(a)(1)	IDENTIFIKOVAT	ID.AM-5 ID.AM-6	7.1	A6.1.1	A5.2
Vrcholové vedení zavede a podporuje politiku bezpečnosti informací a prokazuje základní porozumění tomuto nařízení	Řízení	IS.I.OR.240(a)(2) &(a)(3)	IDENTIFIKOVAT	ID.GV-1	5.1 5.2 7.4	A5.1.1 A7.2.1 A7.2.2	A5.1 A5.4 A6.3
			CHRÁNIT	PR.AT-1 PR.AT-4			
Jmenovat odpovědnou osobu nebo skupinu osob s příslušnými znalostmi k řízení souladu s tímto nařízením	Řízení	IS.I.OR.240(b) IS.I.OR.240(c) IS.I.OR.240(d)	IDENTIFIKOVAT	ID.AM-6 ID.GV-2	7.1 7.2	A6.1.1 A7.2.1 A7.2.2	A5.2 A5.4 A6.3
			CHRÁNIT	PR.AT-1 PR.AT-4			
Vytvořit a udržovat příručku pro řízení bezpečnosti informací (ISMM)	Řízení	IS.I.OR.250			7.5.1	A6.1.3 A12.1.1	A5.5 A5.37
Vypracovat postup, jak příslušnému úřadu	Řízení	IS.I.OR.255(a)	IDENTIFIKOVAT	ID.AM-3	7.4 7.5.1	A6.1.3 A13.2.1 A13.2.2	A5.5 A5.14

Hlavní úkol dle Části IS	Typ činnosti	Reference					
	Řízení, Provozní	Část IS	NIST CSF verze 1.1		ISO/IEC 27001		
			Funkce	Kategorie	Ustanovení odstavce	Annex A Control	
						:2013	:2022
oznamovat změny ISMS							
Řídit změny ISMS a oznamovat příslušnému úřadu změny a/nebo požádat o jejich schválení	Řízení	IS.I.OR.255(a) IS.I.OR.255(b)	IDENTIFIKOVAT	ID.AM-3	7.4	A6.1.3 A13.2.1 A13.2.2	A5.5 A5.14

Dodatek III
Příklady leteckých služeb

Níže je uveden nevyčerpávající a neúplný seznam leteckých služeb, které lze použít jako základ pro identifikaci rozsahu posuzování rizik pro organizaci.

poskytovatel letištních ATM-MET služeb
služba letecké digitální mapy
AIM (externí)
letiště
APP ACC
ATC (externí)
ATC superior
ATM
poskytovatel služeb ATM-MET
operační středisko civilních AU (uživatelů vzdušného prostoru)
komunikační infrastruktura
ER ACC
integrátor dat FIS/TIS
národní AIM
navigační infrastruktura – pozemní
navigační infrastruktura – družicová
poskytovatel služeb jiných než ATM-MET
neletečtí uživatelé (externí)
regionální AIM
regionální ASM
regionální ATFCM
operační středisko státních AU (uživatelů vzdušného prostoru)
služba statických leteckých dat
poskytování společné subregionální služby DCB
subregionální/místní ATFCM

subregionální/národní ASM
přehledová infrastruktura letištní
přehledová infrastruktura traťová
přehledová infrastruktura TMA
časová reference (externí)
věž (TWR)