Systém řízení dle pravidel EU

NCC a SPO provozovatelé

(nesložité organizace)

Úřad pro civilní letectví

Verze 02 – aktualizováno k 16.02.2017

Obsah

Úvod **3**

Politika a cíle bezpečnosti **8**

Řízení bezpečnostních rizik **16**

Zajišťování bezpečnosti **31**

Prosazování (podpora) bezpečnosti **37**

Jak mohu zavést účinný SMS? **39**

Příklady **40**

GAP analýza 41

Politika bezpečnosti 42

Organizační struktura 43

Evidence rizik 44

Obsah SMS příručky 45

Formulář bezpečnostního hlášení 46

Stanovení cílů a ukazatelů výkonnosti (SPI) v bezpečnosti 49

Odkazy **50**

Úvod

Tento materiál by měl sloužit jako průvodce požadavky na systém řízení pro provozovatele zapojené do neobchodního a zvláštního provozu, kteří jsou považováni za tzv. **nesložitou organizaci**.

Je záměrně cílen na „malé(nesložité)“ organizace, které se s tímto konceptem přístupu k bezpečnosti letového provozu dosud nesetkaly a měl by jim pomoci zavést účinný a dobře fungující systém řízení (bezpečnosti).

Nicméně je nutné si uvědomit, že provozovatel musí vždy vycházet zejména z příslušných předpisových požadavků (nařízení (EU) č. 965/2012, Část-ORO) a přijatelných způsobů průkazu (AMC) a výkladového materiálu (GM) uveřejněného agenturou EASA.

Sytém řízení bezpečnosti (SMS) nebo Systém řízení?

Mezinárodní organizace pro civilní letectví (ICAO) postupně od roku 2010 zavádí nový koncept přístupu k bezpečnosti u poskytovatelů služeb v civilním letectví a nazývá jej **Systém řízení bezpečnosti** (Safety Management System (SMS)).

Legislativa EU používá pojem **Systém řízení** (Management System), nicméně se jedná pouze o změnu názvosloví oproti ICAO. Mluvíme o stejném konceptu, stejném přístupu k bezpečnosti letového provozu, jen je jinak nazýván.

V tomto materiálu budeme používat známější pojem Safety Management System (SMS).

Úvod
(Bezpečnost - základní pojmy)

Bezpečnost (Safety)
Stav, při kterém jsou rizika spojená s leteckými činnostmi souvisejícími s provozem letadel nebo jej přímo podporujícími snížena a řízena na přijatelné úrovni.

Systém řízení (bezpečnosti) ((Safety) management system)
Systematický přístup k řízení bezpečnosti zahrnující nezbytné organizační struktury, odpovědnosti, zásady a postupy.

Bezpečnostní riziko (Safety risk)
Předpovídaná pravděpodobnost a závažnost následků nebo výsledků nebezpečí.

Úvod
(Proč potřebuji SMS?)

Předpisový pohled

Zavedení systému řízení je požadováno nařízením (EU) č. 965/2012, Částí-ORO pro provozovatele:

- obchodní letecké dopravy (CAT);
- zvláštního obchodního provozu (SPO);
- zvláštního neobchodního provozu se složitými motorovými letadly (SPO);
- neobchodního provozu se složitými motorovými letadly (NCC).

Praktický pohled

SMS dovoluje provozovateli přijímat opatření k průběžnému zvyšování bezpečnosti svého provozu, prostřednictvím určování nebezpečí, sběru a rozboru údajů o bezpečnosti a průběžným vyhodnocováním bezpečnostních rizik.

Pomáhá lépe pochopit související nebezpečí a rizika a tím předcházet vzniku událostí v letovém provozu (leteckým nehodám a incidentům). SMS je také účinným nástrojem pro zajištění shody s předpisovými požadavky.

Úvod
(„NESLOŽITÁ ORGANIZACE“ z pohledu SMS)

Faktory, které by měly být zohledněny při určování, zda je organizace provozovatele považována za „nesložitou“:

- počet zaměstnanců;
- počet a složitost provozovaných typů letadel;
- počet provozních základen;
- počet letů za dané období;
- počet oprávnění a povolení, kterých je provozovatel držitelem (např. zvláštní oprávnění dle Části-SPA, povolení k vysoce rizikovému SPO);
- provozní prostředí.

AMC1 ORO.GEN.200(b)

Organizace provozovatele by měla být považována za složitou, pokud má pracovní sílu odpovídající více než ekvivalentu 20 zaměstnanců na plný pracovní úvazek, která je zapojena do činností podléhajících nařízení (ES) č. 216/2008 a jeho prováděcím pravidlům.

Organizace provozovatele s personálem zapojeným do činností podléhajících nařízení (ES) č. 216/2008 a jeho prováděcím pravidlům do ekvivalentu 20 zaměstnanců na plný pracovní úvazek mohou být taktéž považovány za složité na základě posouzení následujících faktorů:

(1) z pohledu složitosti – míra a škála dodavatelsky zajišťovaných činností podléhajících schválení;

(2) z pohledu rizikovosti – zda je přítomno něco z následujícího:

(i) provoz vyžadující následující zvláštní oprávnění: provoz s využitím navigace založené na výkonnosti (PBN), provoz za podmínek nízké dohlednosti (LVO), provoz dvoumotorových letounů se zvětšenou vzdáleností od přiměřeného letiště (ETOPS), provoz s vrtulníkovým jeřábem (HHO), provoz vrtulníkové letecké záchranné služby (HEMS), provoz s využitím systému snímání nočního vidění (NVIS) a přeprava nebezpečného zboží (DG);

(ii) zvláštní obchodní provoz vyžadující povolení;

(iii) použití různých typů letadel;

(iv) prostředí (provoz mimo pevninu (offshore), horské oblasti atd.).

Úvod
(Struktura SMS)

4 komponenty	12 prvků
Politika a cíle bezpečnosti	• Závazek a odpovědnost vedení • Odpovědnost za bezpečnost • Jmenování klíčového personálu ve vztahu k bezpečnosti • Koordinace plánu reakce v případě nouze • Dokumentace SMS
Řízení bezpečnostních rizik	• Identifikace nebezpečí • Hodnocení a zmírňování rizik
Zajišťování bezpečnosti	• Sledování a měření výkonnosti v oblasti bezpečnosti • Řízení změn • Průběžné zdokonalování SMS
Prosazování (podpora) bezpečnosti	• Výcvik a vzdělávání • Komunikace o bezpečnosti

Politika a cíle bezpečnosti
(Závazek a odpovědnost vedení 1)

- Účinný SMS vyžaduje dostatek času a přidělení dostatečných zdrojů (lidských i finančních). To vyžaduje, aby vrcholové vedení organizace přijalo závazek a odpovědnost za SMS.
- Tento závazek by měl být vyjádřen v písemné politice bezpečnosti. Tato politika by měla obsahovat jasné směřování SMS s ohledem na účinné udržování vysoké míry bezpečnosti a měla by být podporována odpovědným vedoucím. S politikou bezpečnosti dané organizace musí být seznámen veškerý její personál (politika bezpečnosti musí být zpracována tak, aby byla pro všechny zaměstnance pochopitelná).
- Politika bezpečnosti má být podepsána odpovědným vedoucím, který by měl aktivně projevovat svůj závazek vhledem k bezpečnosti. Takový přístup napomáhá k zavedení politiky „Just Culture“ v rámci organizace.

Just Culture (rovnováha mezi bezpečností a odpovědností)

Je taková kultura „spravedlivého posuzování“ uvnitř organizace, kdy nejsou vedoucí pracovníci, klíčový personál a další zaměstnanci postihováni za činnosti, které vykonávají, opomenutí a svá rozhodnutí odpovídající jejich zkušenostem a výcviku, ale kdy nejsou tolerovány hrubá nedbalost, úmyslné a vědomé porušení pravidel nebo destruktivní činnost.

Tato kultura přispívá k dobrovolnému systému hlášení událostí, kdy ohlašovatel nemusí mít obavy, že bude obviňován ze skutečností, které ohlašuje.

Při zavedení tohoto konceptu by měl být za bezpečnost odpovědný každý zaměstnanec, přičemž by si měl uvědomovat dopady všech svých činností na bezpečnost.

Politika a cíle bezpečnosti
(Závazek a odpovědnost vedení 2)

- Každá politika bezpečnosti bude individuální dle zaměření vaší organizace, nicméně by měla alespoň:
  - v základních rysech popsat váš přístup k bezpečnosti;
  - obsahovat závazek vrcholového vedení ve vztahu k bezpečnosti;
  - obsahovat závazek za poskytnutí odpovídajících zdrojů k udržení účinného systému bezpečnosti a omezení rizik na přijatelnou úroveň;
  - podporovat veškerý personál, aby se aktivně zapojoval do všech prvků SMS a naplňoval je; a
  - podporovat kulturu spravedlivého posuzování (Just Culture) v rámci organizace.

Příklad politiky bezpečnosti pro nesložité organizace je uveden na konci tohoto dokumentu.

Politika a cíle bezpečnosti
(Odpovědnost za bezpečnost 1)

- Odpovědnosti mají být jasným způsobem stanoveny v rámci organizační struktury vaší společnosti. U nesložitých organizací může být tato struktura velice jednoduchá a měla by zejména zahrnovat osobu **odpovědného vedoucího, pracovníky vedení organizace a další klíčové pracovníky, kteří se podílejí na každodenním řízení organizace**. **Některé vedoucí funkce mohou být slučovány**.
- Odpovědnosti odpovědného vedoucího a klíčových pracovníků musí být jasně srozumitelné veškerému personálu organizace.

- **Odpovědný vedoucí má být osoba, která má konečnou odpovědnost za bezpečnost a je zapojena do každodenního řízení organizace**. Základním předpokladem pro dobře fungující SMS je to, že odpovědný vedoucí má pravomoci a finanční kontrolu, které mu umožní přijímat rozhodnutí související s bezpečností a odpovídající opatření, která udrží vysokou míru bezpečnosti v organizaci.

Příklad organizační struktury pro nesložité organizace je uveden na konci tohoto dokumentu.

Politika a cíle bezpečnosti
(Odpovědnost za bezpečnost 2)

- Odpovědnost za otázky(úkoly) související s bezpečnosti může být přidělena dle potřeb organizace, **nicméně konečná odpovědnost za bezpečnost zůstává vždy na odpovědném vedoucím**;
- Nesložité organizace by měly v rámci organizační struktury vyznačit pozice klíčového personálu s jejich odpovědnostmi a zároveň veškeré vazby odpovědnosti v rámci organizace.

Politika a cíle bezpečnosti

(Jmenování klíčového personálu ve vztahu k bezpečnosti)

- Vaše organizace by měla jmenovat **vedoucího bezpečnosti** (kontaktní osoba za SMS). U nesložitých organizací může být tento úkol svěřen odpovědnému vedoucímu nebo jím může být pověřen některý člen personálu.
- V závislosti na velikost vaší organizace může být činnost vedoucího bezpečnosti podpořena dalším personálem organizace v rámci tzv. **výboru pro bezpečnost** (safety committee). Do tohoto výboru mohou být zapojeni i příslušní pracovníci organizací, se kterými spolupracujete v rámci své činnosti.

- Vedoucí bezpečnosti by měl být jedinou kontaktní osobou za SMS (vzhledem k vývoji, administraci a udržování funkčního SMS) a v případě, že se nejedná zároveň o odpovědného vedoucího, **měl by mít k němu přímý přístup**.
- **Dále je důležité, aby se osoby odpovědné za bezpečnost ve vaší organizaci setkávaly a řešily otázky související s bezpečností pravidelně**.

Politika a cíle bezpečnosti
(Koordinace plánu reakce v případě nouze 1)

- **Plán reakce v případě nouze** (ERP – Emergency Response Plan) má popsat opatření, které musí personál přijmout v případě nouze. Minimálně by měl popsat postupy pro:
  - řádný přechod z normálního na nouzový provoz;
  - určení základních pravomocí v případě nouze (ale i např. kdo přebírá pravomoci mimo pracovní dobu nebo o víkendech);
  - přidělení odpovědností v případě nouze (vzájemné zastupování);
  - koordinaci se složkami určenými pro zvládání nouze (kdo je odpovědný za oznámení případu nouze záchranným složkám);
  - bezpečné pokračování provozu nebo bezpečný návrat k normálnímu provozu jakmile je to možné.
- ERP by měl určovat odpovědnosti, role jednotlivého dotčeného personálu a opatření, která mají být přijata v případě nouze. Měl by také zohledňovat všechny dotčené smluvní organizace a dodavatele.
- ERP by měl být součástí samostatného dokumentu. V případě, že máte podobné postupy již vypracovány na základě stávajících požadavků, můžete je i nadále využívat (zajistěte případně jejich revizi, aby byly v souladu s novou legislativou EU).

Politika a cíle bezpečnosti
(Koordinace plánu reakce v případě nouze 2)

- **ERP by měl být dostupný a srozumitelný veškerému dotčenému personálu**. Jeho znalost by měla být pravidelně ověřována, aby si každý uvědomoval své odpovědnosti, pravomoci a opatření související s případem nouze.
- Je důležité koordinovat váš ERP s organizacemi, se kterými spolupracujete nebo s nimi máte uzavřenou smlouvu. Doporučuje se, aby jste s vaším ERP seznámili i dotčené záchranné složky.
- Pro podporu všech dotčených členů vašeho personálu můžete vytvořit karty nebo kontrolní seznamy s příslušnými telefonními kontakty, které jim pomohou při přijímání požadovaných opatření v případě nouze.

Politika a cíle bezpečnosti
(Dokumentace SMS)

- SMS může být zdokumentován v samostatné SMS příručce, nebo může být začleněn do již existujících příruček (např. do provozní příručky).
- Dokumentace může být vedena v papírové formě, ale i elektronicky. Veškeré změny musí být řízeny a systém dokumentace musí zajistit spolehlivost, zálohu (pro obnovení) a ochranu informací proti poškození nebo nechtěné změně.
- Dokumentace SMS má zahrnovat alespoň:
  - politiku a cíle SMS;
  - odpovědnosti klíčových pracovníků a odpovědného vedoucího;
  - jakékoliv procesy, postupy a kontrolní seznamy související s bezpečností;
  - výsledky bezpečnostních auditů a hodnocení, včetně následných opatření z nich vyplývajících;
  - knihovnu rizik; a
  - další informace uvedené v bodě AMC 1 ORO.GEN.200(a)(5) k AMC a GM k Části-ORO (pracovní české znění naleznete zde - http://www.caa.cz/predpisy/amc-a-gm-letovy-provoz)

Příklad obsahu SMS příručky je uveden na konci tohoto dokumentu.

Řízení bezpečnostních rizik
(Jak začíná celý proces?)

1

IDENTIFIKACE NEBEZPEČÍ

(ovlivňující bezpečnost vaší organizace)

2

POSOUZENÍ SOUVISEJÍCÍHO RIZIKA z pohledu:

PRAVDĚPODOBNOSTI
(Jaká je pravděpodobnost, že k riziku dojde?)

ZÁVAŽNOSTI
(Jak vážné budou následky, pokud se riziko naplní?)

Řízení bezpečnostních rizik

(Jednoduchý proces řízení bezpečnostních rizik)

1 IDENTIFIKACE NEBEZPEČÍ

2 POSOUZENÍ RIZIKA

3 ZMÍRŇUJÍCÍ OPATŘENÍ

Pokud je určena úroveň rizika, mohou být zavedena vhodná zmírňující opatření, která úroveň rizika sníží na co nejnižší a prakticky možnou.

4 SLEDOVÁNÍ VÝVOJE

Veškerá zmírňující opatření musí být poté průběžně sledována. Zajistí se tak dosažení požadovaného efektu.

Řízení bezpečnostních rizik
(NEBEZPEČÍ versus RIZIKO)

TEORETICKÝ POHLED

Nebezpečí – podmínky, události nebo okolnosti, které mohou potenciálně způsobit zranění lidí nebo poškození letadla, jeho vybavení nebo konstrukce.

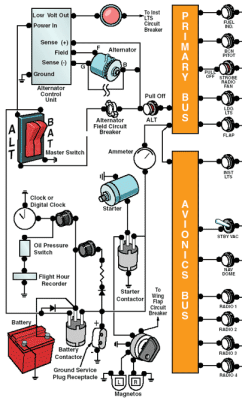
Riziko – je možný výsledek nebezpečí, který je obvykle vyjadřován z pohledu pravděpodobnosti a závažnosti následků nebezpečí.

PRAKTICKÝ POHLED

NEBEZPEČÍ

RIZIKO

NÁSLEDEK



vysazení nebo poškození elektrického systému letadla

Řízení bezpečnostních rizik
(Systém hlášení)

- Nebezpečí může být řízeno pouze pokud je známé. Jeho identifikace může být podpořena prostřednictvím důvěrného **systému bezpečnostního hlášení**. Bezpečnostní hlášení, stejně jako celý proces řízení bezpečnostního rizika, může být:
  - ***reaktivní*** (z událostí, které se staly);
  - ***proaktivní*** (z potencionálních nebezpečných situací, které byly identifikovány); a
  - ***prediktivní*** (snaha o předvídání událostí, které by se mohly stát v budoucnu).
- Organizace by měly podporovat vytvoření **interního dobrovolného systému hlášení**, který by měl zahrnovat především hlášení méně závažných incidentů, které nejsou zahrnuty do systému povinných hlášení vyžadovaného příslušnou legislativou => takový systém vám umožní lépe sledovat výkonnost vaší společnosti v oblasti bezpečnosti a také lépe určovat vývoj vašeho SMS.
- Systém hlášení musí být jasný veškerému personálu vaší i partnerské organizace, všichni musí vědět:
  - **JAK** hlásit;
  - **CO** hlásit;
  - **KDO** podává hlášení;

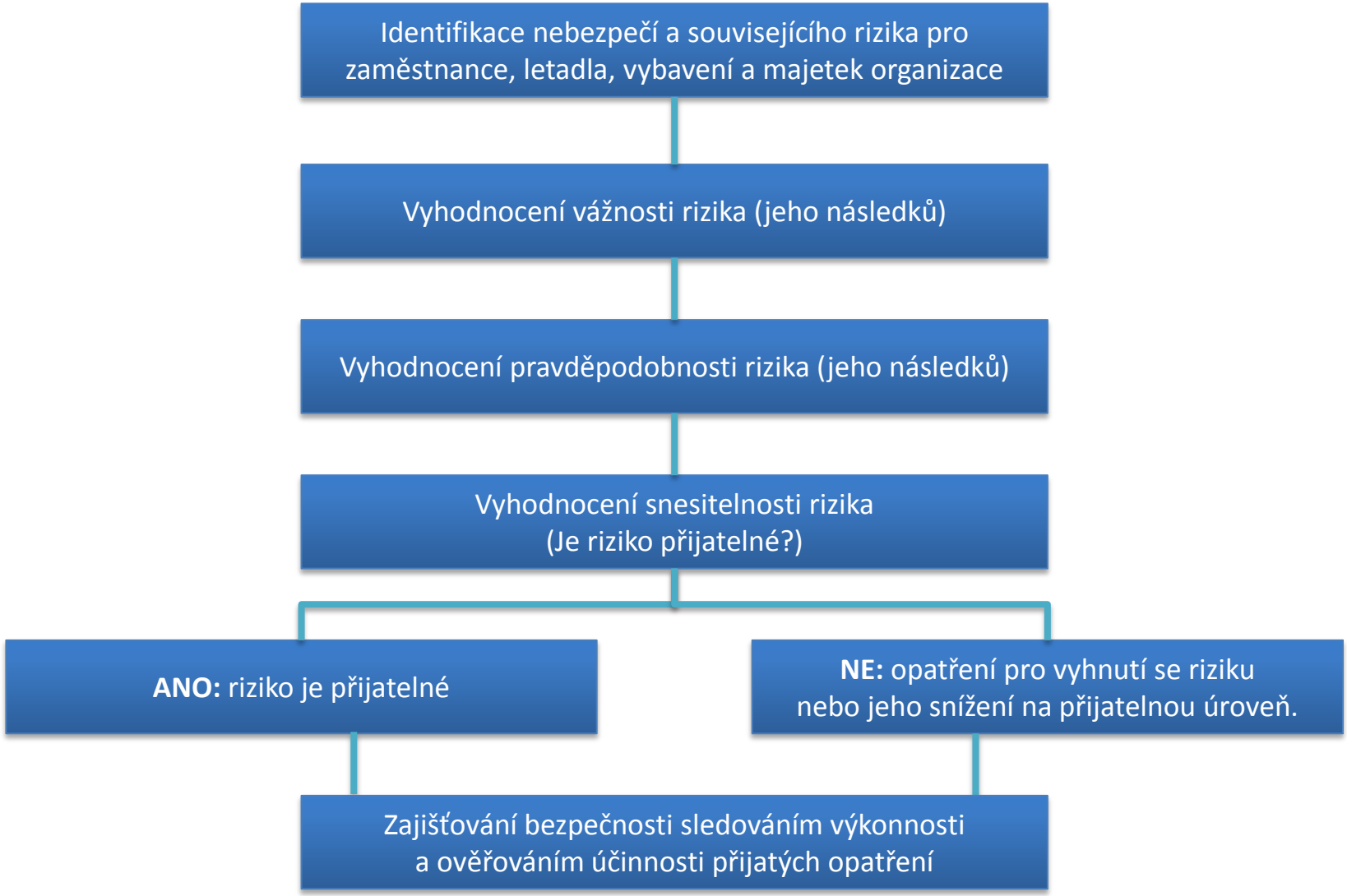
Řízení bezpečnostních rizik
(Identifikace nebezpečí)

- **Proces identifikace nebezpečí** – je metodický a trvalý proces sběru, zaznamenávání a rozboru údajů o nebezpečí, které ovlivňuje činnost vaší organizace. Vše musí být také podpořeno vhodnou zpětnou vazbou ze všech událostí.
- Je mnoho způsobů jak identifikovat nebezpečí a jeho volba záleží i na velikosti vaší organizace, nicméně následující metody by mohly být použitelné:
  - diskuze (tzv. brainstorming) o možných nebezpečích, vedená v rámci výboru pro bezpečnost (pokud je ve vaší organizaci zaveden) nebo malé skupiny určených zaměstnanců;
  - rozbor údajů z předchozích leteckých nehod/incidentů;
  - využívání systémů dobrovolných/povinných hlášení (vnitřních i externích);
  - provádění bezpečnostních hodnocení/auditů (vnitřních i externích);
  - využívání bezpečnostních informací z vnějších zdrojů (např. od podobně zaměřených organizací, z odborných médií, od národních leteckých úřadů, apod.);
  - vytváření **kontrolních seznamů souvisejících s jednotlivými nebezpečími**;
  - …

Řízení bezpečnostních rizik
(Obecné shrnutí)

- **Identifikace nebezpečí není jednorázový proces**. Musí být proveden vždy, když ve vaší organizaci dochází ke změnám, začínáte používat nové vybavení nebo postupy, zavádíte nový druh provozu, došlo ke změně na pozicích klíčových pracovníků a nebo kdykoliv si myslíte, že existuje možnost nového rizika.
- Do procesu hodnocení rizik musí být zahrnuty osoby s dostatečnými znalostmi a zkušenostmi. Veškeré posuzování rizik závisí na kvalitě použitých informací a znalostech osob, které jej provádějí.
- **Podpora zaměstnanců k hlášení možného nebezpečí**, prostřednictvím dobrovolného interního systému hlášení, který je spravedlivý, důvěrný, jednoduchý a uživatelsky přátelský. Takový systém by měl zabránit tomu, že jsou zaměstnanci postihováni za neúmyslné nebo nevědomé chyby nebo selhání (princip „just culture“).
- Je také důležité, aby byla osobě, která hlášení podává, poskytnuta odpovídající zpětná vazba.

Řízení bezpečnostních rizik
(Jednoduchý proces řízení rizik)



Řízení bezpečnostních rizik
(Hodnocení rizik podle VÁŽNOSTI)

- „Pokud se něco stane, jak zlé to bude?“
- Při hodnocení rizik podle závažnosti byste měli zohlednit dosud zavedená zmirňující opatření a vážnost hodnotit s ohledem na nejhorší reálný scénář dané události.
- Při hodnocení rizik podle vážnosti si můžete například položit následující otázky:
  - Mohlo by dojít ke ztrátám na životech (zaměstnanců, cestujících, specializovaných odborníků)?
  - Jaká bude pravděpodobná míra poškození majetku a finanční škody?
  - Jaká bude pravděpodobná míra poškození životního prostředí?
  - Mohlo by dojít ke ztrátě pověsti vaší organizace?
  - …

- Na následující stránce je uveden příklad tabulky pro hodnocení rizik dle vážnosti (nicméně můžete použít i jiný způsob hodnocení).

Řízení bezpečnostních rizik
(Hodnocení rizik podle VÁŽNOSTI)

Vážnost	Význam	Hodnota
Katastrofická	Letecká nehoda, smrt nebo úplné zničení zařízení	A
Nebezpečná	Vážné zranění nebo významné poškození zařízení	B
Závažná	Vážný incident nebo zranění	C
Méně závažná	Méně závažný incident	D
Zanedbatelná	Malé následky	E

Řízení bezpečnostních rizik
(Hodnocení rizik podle PRAVDĚPODOBNOSTI)

- „Jaká je pravděpodobnost, že k riziku dojde?“
- Při hodnocení rizik podle pravděpodobnosti byste měli opět zohlednit dosud zavedená zmirňující opatření. Kromě pravděpodobnosti můžeme také hovořit o četnosti dané události.
- Při hodnocení rizik podle pravděpodobnosti si můžete například položit následující otázky:
  - Došlo již v minulosti k události, která je podobná té, kterou posuzujeme nebo hodnotíme ojedinělou událost?
  - Může dojít u jiného vybavení nebo komponentu stejného typu k podobné poruše?
  - Kolik zaměstnanců se musí řídit dotčenými postupy?
  - Jak dlouho (čas vyjádřený procenty) se „nedůvěryhodné“ vybavení nebo postup používá?
  - …

- Na následující stránce je uveden příklad tabulky pro hodnocení rizik dle pravděpodobnosti (nicméně můžete použít i jiný způsob hodnocení).

Řízení bezpečnostních rizik
(Hodnocení rizik podle PRAVDĚPODOBNOSTI)

Pravděpodobnost (četnost) události	Význam	Hodnota
Častá	Pravděpodobně k ní dojde velmi často	5
Občasná	Pravděpodobně k ní někdy dojde (ne příliš často)	4
Vzdálená (časově)	Není pravděpodobné, že k ní dojde, ale možné to je	3
Nepravděpodobná	Velmi nepravděpodobné, že by k ní došlo (nebo k němu ještě nedošlo)	2
Extrémně nepravděpodobná	Téměř nepředstavitelné, že by k ní došlo	1

Řízení bezpečnostních rizik

(Matice hodnocení bezpečnostních rizik – snesitelnost rizika)

- Pokud jste definovali vážnost a pravděpodobnost rizik, můžete sestavit matici hodnocení bezpečnostních rizik, která vám umožní posoudit **jak snesitelné je toto riziko**.

Pravděpodobnost rizika	**Vážnost rizika**				
	Katastrofická **A**	Nebezpečná **B**	Závažná **C**	Méně závažná **D**	Zanedbatelná **E**
Častá **5**	**5A**	**5B**	**5C**	**5D**	**5E**
Občasná **4**	**4A**	**4B**	**4C**	**4D**	**4E**
Vzdálená (časově) **3**	**3A**	**3B**	**3C**	**3D**	**3E**
Nepravděpodobná **2**	**2A**	**2B**	**2C**	**2D**	**2E**
Extrémně nepravděpodobná **1**	**1A**	**1B**	**1C**	**1D**	**1E**

Řízení bezpečnostních rizik
(Klasifikace snesitelnosti rizika)

- Na základě matice hodnocení bezpečnostních rizik může být **snesitelnost rizika** klasifikována takto:
  - **Nepřijatelné riziko** – pokud je riziko vyhodnoceno takto, činnost by měla být okamžitě zastavena nebo by neměla být zaváděna do provozu. Musí být přijata významná opatření pro zmírnění rizika na úroveň *tak nízkou jak je přiměřeně možné (ALARP – As Low As Reasonably Practicable)*;
  - **Snesitelné riziko** – v tomto případě by měla být přijata další opatření pro zmírnění rizika na úroveň ALARP. Je nutné i nadále tato rizika sledovat a vyhodnocovat jejich vážnost a pravděpodobnost. Pokud i po přijetí zmírňujících opatření činnost spadá do této oblasti snesitelnosti může být další přijímání zmirňujících opatření zastaveno (např. z důvodu vysokých finančních nákladů na ně) pod podmínkou, že je tomuto riziku porozuměno a je odsouhlaseno odpovědným vedoucím;
  - **Přijatelné riziko** – v tomto případě, je následek rizika nepravděpodobný nebo není tak vážný. Nicméně je nutné rizika stále sledovat a případně zavádět další zmírňující opatření.

Řízení bezpečnostních rizik
(Zmírňování rizik)

- Opatření pro zmírňování rizik představují činnosti nebo změny, např. v provozních postupech, vybavení nebo infrastruktuře organizace, které sníží pravděpodobnost a/nebo vážnost rizika.
- Obecně je možné přístup pro zmírnění rizik rozdělit do 3 kategorií:
  - **Vyhýbání se riziku:** provoz nebo činnost jsou zrušeny nebo se jim organizace vyhýbá, jelikož bezpečnostní riziko vysoce převyšuje přínos takového provozu nebo takové činnosti;
  - **Omezení rizika:** četnost daného provozu nebo činnosti je snížena nebo jsou přijata opatření ke snížení závažnosti následků rizika;
  - **Izolace rizika:** jsou přijata opatření pro izolaci následků rizika nebo opatření, která danou činnost před rizikem chrání.

Řízení bezpečnostních rizik
(Evidence rizik)

- Součástí dokumentace vašeho SMS by měla být také **evidence rizik nebo záznam zjištěných nebezpečí**. Tato dokumentace by měla obsahovat:
  - každé identifikované nebezpečí;
  - související rizika;
  - výsledky hodnocení rizik (při zohlednění stávajících zmírňujících opatření);
  - další přijatá opatření ke zmírnění rizik (pokud bylo nutné je přijmout na základě posouzení);
  - opětovné hodnocení rizik (ověření účinnosti přijatých opatření k jejich zmírnění).
- Tento dokument by měl být pravidelně přezkoumáván (zejména během jednání výboru pro bezpečnost nebo podobné skupiny ve vaší organizaci).

*Příklad evidence rizik pro nesložité organizace je uveden na konci tohoto dokumentu. Další příklad můžete nalézt v AMC a GM k Části-ORO, bodu **GM3 ORO.GEN.200(a)(3)**.*

Zajišťování bezpečnosti
(Úvod)

- Proces zajišťování bezpečnosti (ověřování její úrovně) slouží ke sledování výkonnosti vaší organizace v oblasti bezpečnosti a účinnosti vašeho SMS.
- Tímto procesem by mělo být zajištěno, že identifikace nebezpečí, posouzení rizik a navržení zmírňujících opatření bylo provedeno efektivně a že tato opatření byla zavedena, jsou účinná a dobře fungují.

Proces zajišťování bezpečnosti vám dává jistotu, že **zavedená zmírňující opatření pro všechna identifikovaná nebezpečí jsou účinná a bylo dosaženo požadovaných cílů v oblasti bezpečnosti**.

Zajišťování bezpečnosti
(Sledování a měření výkonnosti v oblasti bezpečnosti 1)

- Pro řízení výkonnosti v oblasti bezpečnosti je důležité její měření a k tomu potřebujete údaje o bezpečnosti. Míru bezpečnosti vaší organizace můžete změřit pomocí tzv. **ukazatelů výkonnosti v bezpečnosti** (SPI – Safety Performance Indicators).
- Jaké SPI použijete závisí na konkrétní organizaci a úrovni údajů o bezpečnosti, které máte k dispozici (obecný návod je uveden v části příklady).
- Mezi zdroje údajů o bezpečnosti, které lze použít jako SPI, můžete zahrnout např.:
  - hlášení nebezpečí a incidentů;
  - hlášení a podněty zákazníků;
  - povinná hlášení událostí;
  - průzkumy zákazníků a smluvních partnerů; a
  - nálezy z bezpečnostních průzkumů a auditů.

Zajišťování bezpečnosti
(Řízení změn)

- Každá změna ve vaší organizaci (nové letadlo, nové vybavení, nová činnost, nové tratě nebo oblasti provozu, nové postupy, apod.) přináší další možné nebezpečí, a proto byste měli zavést jednoduché postupy, které zajistí, že bude každá změna z tohoto hlediska posouzena.
- Měli byste si položit zejména následující otázky:
  - Jsou naše stávající postupy dostatečné nebo je musíme změnit?
  - Absolvoval veškerý personál příslušný výcvik?
  - Vědí organizace, se kterými spolupracujeme o všech našich změnách?

- Proces řízení změn by měl zajistit, že očekávané změny nebudou mít bezpečnostní dopad na stávající nebo budoucí aktivity vaší organizace.

Proces řízení změn by měl využívat stejný přístup jako při běžném posuzování bezpečnostních rizik.

Zajišťování bezpečnosti
(Řízení incidentů)

- K incidentům dochází a je to v podstatě nevyhnutelné. V účinném a dobře fungujícím SMS byste si měli z každého incidentu vzít ponaučení a měli byste bezprostředně přijímat všechny požadované změny a opatření.
- Stanovte si jednoduché postupy pro šetření každého incidentu. Míra šetření samozřejmě bude záviset na závažnosti události.
- V rámci šetření se zaměřte na to: Co se stalo, jak, kdy, kde a kdo byl do incidentu zapojen. Je důležité vždy stanovit fakta a vyhnout se dohadům!

Kromě toho co bylo uvedeno výše se vždy snažte být objektivní – je hlavní zjistit **PROČ** k incidentu došlo, aby se zabránilo tomu, že k němu dojde znovu.

Není vždy nutné zaměřit se pouze na to, kdo incident zavinil.

Sdílejte informace o incidentech se svými zaměstnanci a organizacemi, se kterými spolupracujete => ponaučení.

Zajišťování bezpečnosti
(Průběžné zdokonalování SMS 1)

- Vhodným nástrojem pro průběžné zdokonalování vašeho SMS, který zajistí, že váš systém nezůstane statickým, ale bude se dále rozvíjet a tím bude účinný a funkční, je tzv. **systém sledování shody**.
- Takový systém vyžaduje zejména následující:
  - sledujte zda vaše organizace splňuje aktuální předpisové požadavky na SMS;
  - sledujte zda jsou zavedená zmírňující opatření a procesy řízení dostatečná a stále účinná; a
  - průběžné hodnocení postupů a procesů popsaných ve vaší SMS příručce, jak jsou zavedeny a uplatňovány.
- Sledování shody by mělo být uzavřený proces, který zajistí, že jsou zjištěné problémy napraveny. Do systému sledování shody byste měli zahrnout i vaše smluvní a partnerské organizace.

Zajišťování bezpečnosti
(Průběžné zdokonalování SMS 2)

- U nesložitých organizací, v kterých může být do SMS zapojen každý, je vhodné zavést systém nezávislých hodnocení nebo auditů. Což v praxi znamená využití nezávislých externích auditorů nebo organizací.
- Jelikož vám systém sledování shody pomáhá sledovat výkonnost vaší organizace v bezpečnosti, je nezbytné, aby byl do systému zapojen odpovědný vedoucí, sledoval samotný systém a výsledky hodnocení a auditů.
- Způsob sledování shody pro nesložité organizace je uveden v AMC a GM k Části-ORO, v bodu **GM3 ORO.GEN.200(a)(6)**.

Poznámka: informaci o dostupnosti citovaných dokumentů naleznete na stránce Odkazy.

Prosazování (podpora) bezpečnosti
(Výcvik a vzdělávání)

- Každý ve vaší organizaci má odpovědnost za bezpečnost letectví. Je důležité, aby byl veškerý personál schopný zajistit své úkoly a odpovědnosti v oblasti bezpečnosti, což je dosaženo pravidelným výcvikem v oblasti bezpečnosti a průběžným hodnocením všech zaměstnanců.
- Výcvik by měl zejména zahrnovat strukturu vašeho SMS, politiku bezpečnosti vaší organizace, postupy hlášení a odpovědnosti ze bezpečnost u jednotlivých zaměstnanců.

Uchovávejte záznamy každého zaměstnance o absolvování výcviku v bezpečnosti.

Každý zaměstnanec by si měl uvědomovat nebezpečí a bezpečnostní rizika spojená s činností, kterou vykonává.

Využívejte pro potřeby výcviku rozbory incidentů a jejich šetření.

Účinná podpora bezpečnosti vede k tomu, že je každý zaměstnanec vaší organizace schopný aktivně identifikovat a hlásit zjištěné nebezpečí.

Prosazování (podpora) bezpečnosti
(Komunikace o bezpečnosti)

- Sdílení informací o bezpečnosti napříč organizací je velice důležité, zajistí, že veškerý personál vaší organizace bude mít k dispozici informace vztahující se k nebezpečím a rizikům spojených s vaší činností, a dále mu pomůže pochopit zavedení všech postupů a změn s ohledem na bezpečnost ve vaší organizaci.

Jednoduchý způsob jak tyto informace sdílet může představovat:

- pravidelná setkání zaměstnanců;
- bezpečnostní bulletiny, informační letáky a prezentace šířené například prostřednictvím emailu nebo intranetu.

Můžete také zkusit spolupráci v podobnými organizacemi a sdílet vzájemně své zkušenosti a bezpečnostní informace.

JAK mohu zavést účinný SMS?
(GAP analýza a plán zavedení SMS)

- Na předchozích stranách byly uvedeny základní komponenty, které vytváří SMS. Vytvoření účinného SMS vyžaduje čas a prostředky, aby byly všechny uvedené komponenty ve vaší organizaci řádným způsobem zavedeny.
- Některé již ve vašich organizacích fungují a jiné ještě ne. Z tohoto důvodu je dobré, když celý proces zavedení SMS začnete provedením **srovnávací (GAP) analýzy**, která vám řekne, které komponenty již máte zavedené a které ne nebo zda je potřeba již zavedené ještě rozvinout.
- GAP analýza by měla být tvořena hodnotícími otázkami, které se vztahují k jednotlivým komponentům SMS.
- Z uvedené analýzy vám poté vyplyne **plán na zavedení SMS**. Plán by měl stanovit jasný časový rámec a měl by být realistický.

Pamatujte:

- účinný a vyzrálý SMS potřebuje čas, aby mohl být plnohodnotně zaveden; a
- je důležité uvědomit si, že k účinnému SMS může přispět každý zaměstnanec vaší organizace.

Příklady

Na následujících stranách jsou uvedeny příklady a návody pro:

- GAP analýzu;
- Politiku bezpečnosti;
- Organizační strukturu;
- Evidenci rizik;
- Obsah SMS příručky;
- Formulář bezpečnostního hlášení; a
- Stanovení cílů a ukazatelů výkonnosti (SPI) v bezpečnosti.

Jedná se o modelové příklady a návody. Většina dále uvedené dokumentace by měla vždy odpovídat složitosti a velikosti vaší organizace!

Příklady
(GAP Analýza)

Vytvořte si hodnotící tabulku, která bude obsahovat **všechny komponenty a prvky SMS**, které mají být zavedeny a odpovězte si na všechny položené otázky. Tak budete vědět, co je již ve vaší organizaci zavedeno a na čem musíte ještě pracovat!

Číslo	*Co je posuzováno / Otázka na kterou hledáte odpověď*	*Odpověď*	*Stav implementace*
Komponent 1 – POLITIKA A CÍLE BEZPEČNOSTI			
Prvek 1.1 - Závazek a odpovědnost vedení			
1.1-1	Je zpracována politika bezpečnosti?	☐ Ano ☐ Ne ☐ Částečně	
1.1-2	Obsahuje politika bezpečnosti závazek vrcholového vedení ve vztahu k řízení bezpečnosti?	☐ Ano ☐ Ne ☐ Částečně	
1.1-3	Odpovídá politika bezpečnosti velikosti, povaze a složitosti organizace?	☐ Ano ☐ Ne ☐ Částečně	
1.1-3	Je politika bezpečnosti podepsána odpovědným vedoucím?	☐ Ano ☐ Ne ☐ Částečně	
…	…	…	…

Příklady
(Politika bezpečnosti)

Politika bezpečnosti

Zajištění vysoké úrovně bezpečnosti je naším prvotním cílem.

Jako odpovědný vedoucí jsem zodpovědný za zajištění bezpečnosti našeho provozu a všech poskytovaných služeb. Budu zajišťovat poskytování dostatečných zdrojů a výcviku personálu k dosažení účinného systému řízení bezpečnosti.

Podporujeme všechny naše zaměstnance a spolupracující organizace, aby podávali vždy hlášení související s událostmi a nebezpečími ohrožující bezpečnost, i když by mohly být považovány za bezvýznamné. V rámci systému hlášení podporujeme přístup spravedlivého posuzování (just culture).

Zavazujeme se, že:
- budeme budovat a stále rozvíjet účinný systém řízení bezpečnosti;
- budeme dodržovat platné předpisy, standardy a osvědčené postupy;
- budeme podporovat bezpečnost jako primární odpovědnost všech vedoucích pracovníků;
- ….

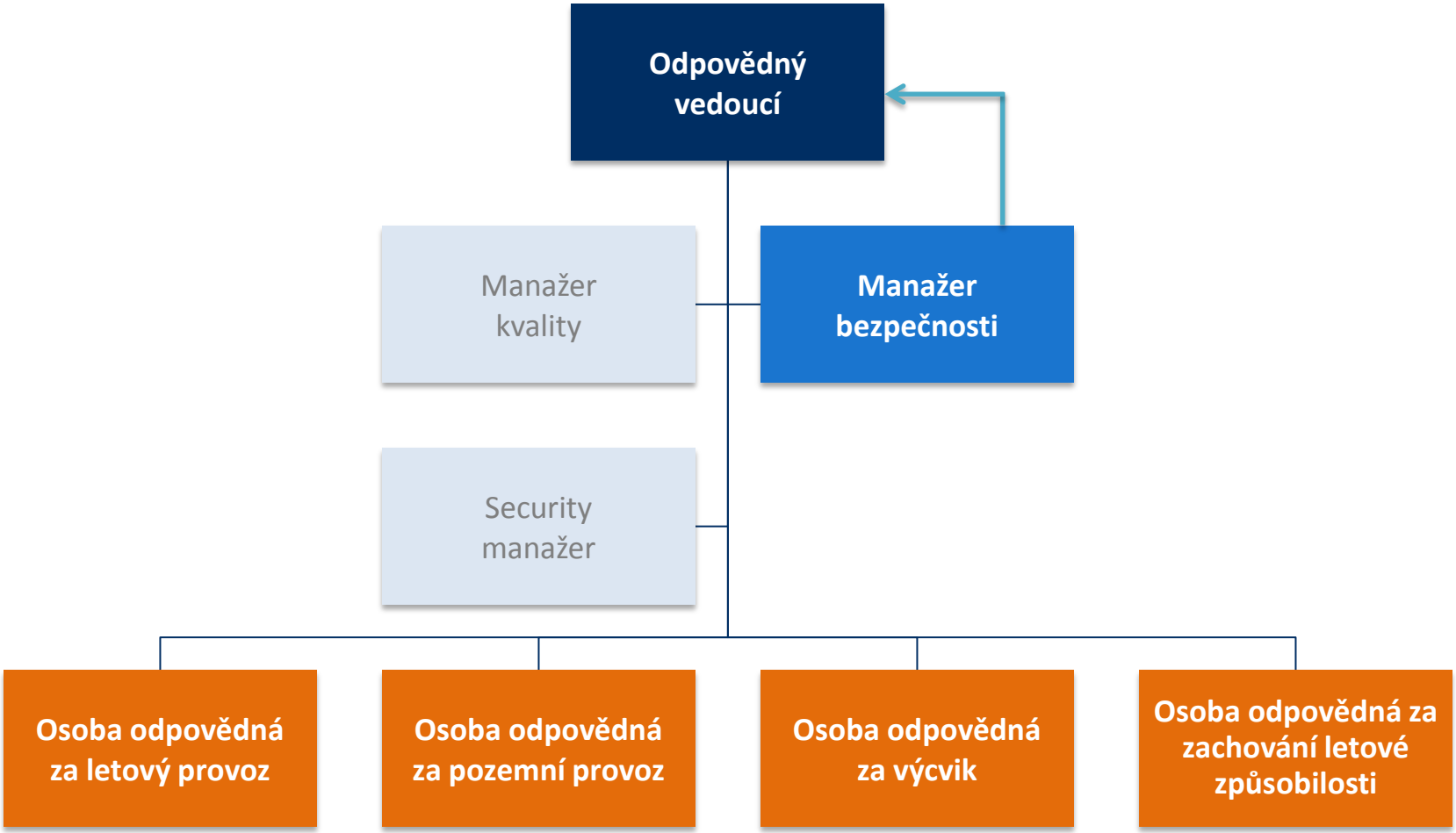
Naše závazky a cíle v bezpečnosti vnímáme jako přínos pro naší společnost, naše zákazníky a veškerou naší činnost. K dosažení těchto cílů využíváme politiku sdílené odpovědnosti.

….

V …… dne ……

……
podpis odpovědného vedoucího

Příklady
(Organizační struktura)



Organizační struktura bude vždy odpovídat složitosti a velikosti vaší organizace.
Funkce uvedené v této struktuře mohou být slučovány.

Příklady
(Evidence rizik)

Identifikované nebezpečí	Související rizika (následky)	Zavedená zmírňující opatření	Stávající úroveň rizika	Další zmírňující opatření	Revidovaná úroveň rizika	Opatření provedl/dne
1. …. 	1. …. 2. ….	1. …. 2. …. 1. …. 2. ….	Vážnost …. Pravděpodobnost … ☐ Přijatelné ☐ Snesitelné ☐ Nepřijatelné	1. …. 1. …. 2. ….	Vážnost …. Pravděpodobnost … ☐ Přijatelné ☐ Snesitelné ☐ Nepřijatelné	

Hodnocení rizika dle vážnosti provedete podle tabulky uvedené **na straně 24**.
Hodnocení rizika dle pravděpodobnosti provedete podle tabulky uvedené **na straně 26**.
Na straně 27 je uvedena **matice hodnocení bezpečnostního rizika**, z které vám dle kombinace vážnosti/pravděpodobnosti vyjde míra úrovně rizika – **přijatelné / snesitelné / nepřijatelné**. Podle této úrovně můžete poté zavést další zmírňující opatření, která vám úroveň bezpečnostního rizika sníží.

Příklady
(Obsah SMS příručky)

1. **Obsah**
2. **Seznam platných stran**
3. **Rozdělovník**
4. **Politika a cíle bezpečnosti**

   [tato část by měla obsahovat politiku bezpečnosti podepsanou odpovědným vedoucím]
5. **Organizace bezpečnosti**

   [tato část by měla podrobně popsat strukturu řízení organizace a:

   (a) *Rozsah SMS a smluvní činnosti* (zde by mělo být popsáno jaké činnosti pokrývá SMS a jak je propojen se smluvními organizacemi (pokud vaše organizace využívá smluvní činnosti));

   (b) *Odpovědnost za bezpečnost* (zde uveďte klíčové zaměstnance související s bezpečností, členy výboru pro bezpečnost, je-li ustanoven, a odpovědnosti všech klíčových pracovníků);

   (c) *Dokumentace SMS* (zde popište způsob dokumentace SMS a vedení záznamů)]
6. **Proces identifikace nebezpečí a řízení rizik**

   [tato část by měla obsahovat popis systému hlášení, identifikace nebezpečí a procesu hodnocení rizika (jak je nebezpečí a související riziko posuzováno a následně řízeno)]
7. **Zajišťování bezpečnosti**

   [tato část by měla obsahovat popis, jak jsou SMS a jeho výstupy kontrolovány (auditovány). Měl by zde být také uveden systém sledování a měření výkonnosti v oblasti bezpečnosti]
8. **Řízení změn**

   [zde popište jak je SMS využíván pro řízení změn ve vaší organizaci]
9. **Plán reakce v případě nouze**

   [tato část by měla popsat jak organizace reaguje na případy nouze a měla by také obsahovat kontrolní seznamy nebo karty uvedené na straně 14]

Příklady
(Formulář bezpečnostního hlášení)

Část A: Vyplní osoba podávající hlášení nebo identifikující nebezpečí

Datum události: ..... Čas: .....

Místo: .....

Jméno osoby podávající hlášení: ..... Funkce: .....

Uveďte úplný popis události nebo zjištěného nebezpečí, včetně návrhu jak předcházet takovým událostem:

Jaká je dle vašeho názoru pravděpodobnost, že k takové nebo podobné události opět dojde?

Extrémně nepravděpodobná *Častá*

1 2 3 4 5

Jak vážné by mohly být dle vašeho názoru možné následky události ke které došlo nebo by k ní došlo znovu?

Zanedbatelné *Katastrofické*

1 2 3 4 5

Příklady
(Formulář bezpečnostního hlášení 2)

Část B: Vyplní osoba odpovědná za bezpečnost ve vaší organizaci (např. vedoucí bezpečnosti)

Hlášení bylo anonymizováno a zapsáno do databáze organizace.

Číslo hlášení: .....

Jméno: ..... Datum: .....

Podpis: .....

Příklady
(Formulář bezpečnostního hlášení 3)

Část C: Vyplní výbor pro bezpečnost (pokud je ve vaší organizace zřízen) nebo vedoucí bezpečnosti

Posouzení pravděpodobnosti události ke které došlo nebo by mohlo dojít?

Extrémně nepravděpodobná				*Častá*
1	2	3	4	5

Posouzení nejhorších následků?

Zanedbatelné				*Katastrofické*
1	2	3	4	5

Opatření přijatá k odstranění, zmírnění nebo řízení nebezpečí k dosažení přijatelné úrovně bezpečnosti:

Požadované zdroje: ..... Odpovědná osoba za přijatá opatření: .....

Místo: .....

Odsouhlaseno a schváleno: Vedoucím bezpečnosti: ..... Datum: .....

Odpovědným vedoucím: ..... Datum: .....

Zaměstnanci(zaměstnancům) byla poskytnuta zpětná vazba vedoucím bezpečnosti.

Podpis: ..... Datum: .....

Navazující opatření: .....

Evidence rizik aktualizována dne: .....

Příklady
(Stanovení cílů a ukazatelů výkonnosti (SPI) v bezpečnosti)

- Jedním z nástrojů, jak stanovit cíle a sledovat výkonnost v oblasti bezpečnosti, může být vytvoření následujícího přehledu:

Ukazatel výkonnosti	**Cíle**	**Výkonnost**											
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
		1. čtvrtletí			**2. čtvrtletí**			**3. čtvrtletí**			**4. čtvrtletí**		
Počet incidentů s vysokým rizikem	1 nebo méně												
Počet událostí podléhajících povinnému hlášení	3 nebo méně												
Počet interních auditů	4												
Počet nálezů z interních auditů	2 nebo méně												
Počet jednání výboru pro bezpečnost	6												
Účast klíčových pracovníků na jednání výboru pro bezpečnost	Min. 80 %												
Počet bezpečnostních hlášení / hlášení o nebezpečí	20 nebo méně												
Počet oficiálních vyhodnocení rizik	5 nebo méně												
Počet incidentů souvisejících s letovou způsobilostí	1												
Počet letů s MEL omezeními	1												
…	….												

Poznámka: Uvedené cíle a ukazatele jsou pouze příklad. Organizace by měla stanovit cíle a ukazatele, které budou odpovídat konkrétnímu druhu provozu.

Odkazy

Předpisy / Přijatelné způsoby průkazu (AMC) a Poradenský materiál (GM)

EUR-LEX (přístup k právu EU)

http://eur-lex.europa.eu/homepage.html?locale=cs

EASA (přístup k AMC a GM)

http://www.easa.europa.eu/document-library/acceptable-means-of-compliance-and-guidance-materials

ÚCL (přístup k nařízením EU a pracovním českým zněním EASA AMC/GM)

http://www.caa.cz/predpisy/zakladni-informace-k-narizenim-eu

http://www.caa.cz/predpisy/prijatelne-zpusoby-prukazu-amc-a-poradensky-material-gm

Informace k bezpečnosti (Safety)

EASA

http://www.easa.europa.eu/easa-and-you/safety-management

ICAO

http://www.icao.int/safety/Pages/default.aspx

http://www.icao.int/safety/SafetyManagement/Pages/default.aspx

OSTATNÍ

https://www.faa.gov/about/initiatives/sms/

https://aviation-safety.net/

https://flightsafety.org/

http://www.skybrary.aero/index.php/Safety_Management_System

https://www.asms-pro.com/SMS.aspx