HOSPODÁŘSKÁ KOMORA ČESKÉ REPUBLIKY

EFEKTIVNÍ ŘÍZENÍ RIZIK V SYSTÉMECH MANAGEMENTU

SÍLA | RESPEKT | NEZÁVISLOST

Vážení členové Hospodářské komory České republiky,

v současné době jsou podnikatelé vystaveni řadě rizikových situací a záleží na tom, zdali je budou řešit intuitivně nebo zvolí plánovanou či řízenou cestu prevence, a budou lépe připraveni řešit ohrožení svého podnikání. S pomocí této příručky snáze proniknete do problematiky řízení rizik a zvládnete připravit své havarijní plány a další opatření, která Vám napomohou zvládat běžně neočekávané situace s větším přehledem. Kolektiv autorů se zaměřil na několik oblastí, ze kterých mohou vzejít závažné zdroje rizik:

- neplnění závazků vůči partnerům a zákazníkům,
- vysoká závislost na technologiích (ERP systémy, klíčové aplikace, robotizovaná pracoviště),
- komplexita procesů a IT systémů a navazující kybernetická kriminalita,
- nízká ochrana vybavení a zařízení, infrastruktury organizace, včetně průmyslové bezpečnosti,
- omezení technickými předpisy a regulatorními kritérii,
- závislost na dodavatelích a poskytovatelích klíčových služeb,
- krizový management a neefektivní komunikace,
- vnější vlivy (omezení zdrojů surovin), environmentální podmínky.

Publikace, která se vám dostává do rukou, byla vypracována týmem odborníků, kteří se zabývají systémy managementu a souvisejícími požadavky na řízení rizik. Vybrali jsme pro vás řadu kritických oblastí, a pomocí osmi krokové metody „Modelu řízení rizik“ si ukážeme, jak rizika posuzovat a včasnou reakcí zabránit jejich negativním dopadům. Publikace je strukturována tak, že v jedné části popisuje každý krok modelu a následně ukazuje, jaké preventivní činnosti lze nastavit pro jednotlivé systémy managementu:

- management kvality podle ISO 9001 (QMS),
- environmentální management podle ISO 14001 (EMS),
- management bezpečnosti práce a ochrany zdraví při práci podle ISO 45001 (OHSMS),
- management bezpečnosti informací podle ISO/IEC 27001 (ISMS),
- management kontinuity podnikání podle ISO 22301 (BCM),
- energetický management podle ISO 50001 (EnMS).

Řízení podnikových rizik představuje dvě oblasti, nastavení systému managementu a zajištění udržitelného podnikání. Průvodce v osmi krocích umožňuje posuzování a řízení rizik, včetně zajištění vhodných havarijních plánů.

K dispozici budou dvě verze Průvodce řízením rizik. Pouze elektronická verze bude obsahovat vzorové postupy a související záznamy.

Kolektiv autorů

Slovník (termíny a definice)

Environmentální aspekt – vliv, důležité hledisko environmentálních systémů.

Havarijní plán – postup zvládání a minimalizování dopadů incidentů, též nouzový plán. V užším významu se může jednat o ochranu vod, prevenci závažných havárií či plán první pomoci.

Hodnocení souladu – vyhodnocení rizika odchylek zákonných požadavků nebo předpisů a norem.

Incident – situace, která může být, nebo by mohla vést k narušení, škodám, stavu nouze nebo krizi.

Interní a externí vlivy – parametr a faktory, které mohou být brány v úvahu pro porozumění podnikatelskému prostředí organizace.

Kapacita rizika (Risk Capacity) – souhrnně vyjádřená hodnota rizika, které organizace může nést, a nad jejíž hranicí je ohroženo udržitelné podnikání.

Krizový management – zabývá se strategickými vlivy a komunikací s médii.

Míra rizika – kombinace pravděpodobnosti výskytu události a jejich dopadu na organizaci.

Model řízení rizik – 8 krokový cyklus pro hodnocení a ošetření rizik.

Nebezpečí – zdroj rizika, újmy či potenciálního poškození.

Nebezpečná situace – okolnosti, za kterých jsou lidé, majetek nebo prostředí vystaveni jednomu nebo více nebezpečím.

Operativní řízení rizik – vyhodnocení finančních ztrát, které jsou způsobeny neadekvátně řízenými systémy či procesy, ale i externími negativními vlivy.

Plán kontinuity podnikání (Business Continuity Plan, BCP) – postup prováděný organizací jako reakce na incident, který umožňuje zahájení provozu na předem definované úrovni po narušení.

Plán obnovy (Recovery Plan, RP) – postup, který stanoví, jak má organizace reagovat, aby se minimalizoval dopad incidentu (katastrofy), a jak co nejrychleji obnovit provoz.

Plány pro stahování produktu z oběhu (Recall Plans) – poskytují návod, kterým výrobce potravin informuje příjemce, jak nakládat s produkty stahovanými z trhu.

Procesní přístup – nastavení procesního řízení organizace, které bude umožňovat řízení rizik a hodnotit efektivnost procesů.

Projektová rizika – rizika dodržení parametrů projektů (doba trvání, náklady, cíle)

Riziko – účinek nejistoty. Příležitost nebo ohrožení v podnikání.

Událost – výskyt nebo změna určité množiny okolností. Událost se může vyskytnout jednou nebo vícekrát a může mít několik příčin. Událost se může někdy nazývat „incident“ či „nehoda“. Událost bez následků se může též nazývat „skoro nehoda“, „incident“, „skoro úspěch“ nebo „uniknutí o vlas“.

Zainteresované strany – subjekty jejichž potřeby a požadavky organizace zahrnuje při naplňování podnikatelských záměrů.

Zvažování rizika – uvažování na základě rizik, vnímání rizik a jejich předvídání všemi pracovníky je nedílnou součástí řešení problémů a rozhodování o přijetí opatření.

Slovník (termíny a definice)

Metody pro analýzy rizik, příklady

- Analýza rizik BOZP – analýzy bezpečnosti práce
- BIA (Business Impact Analysis) – analýza dopadů rizik na podnikání.
- Brainstorming – jednoduchá metoda postavená na týmovém hodnocení
- EIA (Environmental Impact Assessment) – posuzování vlivů na životní prostředí
- ETA (Event Tree Analysis) – analýza stromu událostí
- ERP (Enterprise Resource Planning) – plánování podnikových zdrojů, též kategorie informačního systému
- FMEA (Failure Mode Effect Analysis) analýza potenciálních chyb a jejich dopadů
- FTA (Fault Tree Analysis) – analýza stromu poruchových stavů
- HACCP (Hazard Analysis and Critical Control Points) – analýza rizik a kritické kontrolní body
- HAZOP – analýza rizik provozu-schopnosti technických zařízení
- PEST – analýza externích vlivů, zohledňující politická, ekonomická, sociální a technologická hlediska
- RA (Risk Assessment) – proces posuzování rizik
- RIA (Regulatory Impact Assessment) – hodnocení dopadů regulace
- SWOT – analýza silných a slabých stránek), jednoduchá a frekventovaně používaná analýza
- VA (Vulnerability analysis) – analýza zranitelnosti

Použité zkratky

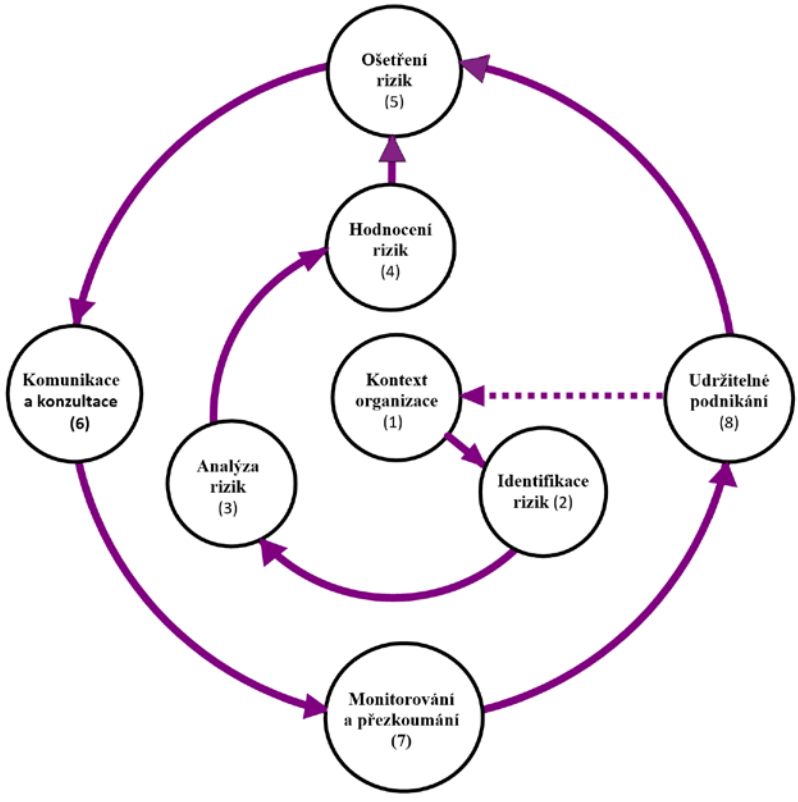
- BCMS (Business Continuity Management System) – systém managementu kontinuity podnikání
- BCP (Business Continuity Plan) – plány kontinuity podnikání
- D-FMEA – designová analýza potenciálních chyb a jejich dopadů
- ERP (Enterprise Resource Planning) – plánování podnikových zdrojů
- ICT – informační a komunikační technologie
- IoT (Internet of Things) – internet věcí
- IT – informační technologie
- KPI (Key Performance Indicator) – klíčový indikátor výkonnosti
- KRI (Key Risk Indicator) – klíčový indikátor míry rizika
- LCA – posuzování životního cyklu
- MAO (Max Acceptable Outage) – maximální akceptovatelný výpadek, doba, po kterou může být systém nebo služba nedostupný/á
- MTPD (Maximum Tolerable Period of Disruption) – maximální přípustná doba narušení
- OOPP – osobní a ochranné pracovní prostředky
- PESTLE – analýza politických, ekonomických, sociálních, technologických, právních a environmentálních hledisek
- P-FMEA – procesní analýza potenciálních chyb a jejich dopadů
- Prevence závažných havárií – zákonný systém pro objekty a zařízení s nebezpečnými chemickými látkami
- RPO (Recovery Point Objective) – cílový bod zotavení, maximální objem ztracených dat
- RTO (Recovery Time Objective) – cílová doba zotavení, časový interval pro obnovení činnosti

Slovník (termíny a definice)

Model pro řízení rizik má 8 postupových kroků. Ve vnitřním kruhu rozhodujeme, kdo a jak bude zapojen do posouzení rizika. Na základě ohodnocení rizik, kdy již známe míru rizika, přecházíme k řízení rizik dle vnějšího kruhu, který představuje program řízení rizik.

Přístup k posouzení rizik – vnitřní kruh určuje potřeby a požadavky osob vstupujících do kontextu organizace (1) a výběr účastníků posuzujících rizika. Následně identifikujeme rizika (2), provádíme jejich analýzy (3) a hodnocení (4) na základě stanovených kritérií.

Program řízení rizik – pomocí vnějšího kruhu krok za krokem promyslíme, jak můžeme ošetřit rizika (5), komunikovat a konzultovat (6) rizikové faktory na úrovni vedení organizace, které je odpovědné za monitorování a přezkoumání rizik (7), aby mohla být zajištěna udržitelnost podnikání (8).



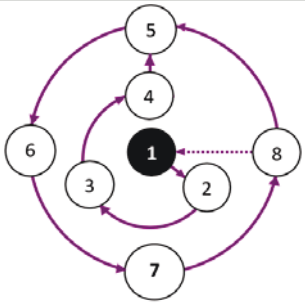
Obrázek 1: Model pro řízení rizik

Od modelu pro řízení rizik podle ISO 31000 se náš přístup liší v rozšíření postupu o 8. krok „Udržitelné podnikání“. Ten organizaci bezprostředně po narušení vede k reakci, následnému zotavení a znovu zahájení provozu. Použití uceleného 8 krokového modelu přispěje k vaší stabilitě a způsobilosti dodávat produkty nebo služby, to vše bez dodatečných nákladů/finančních a jiných ztrát na přijatelné úrovni rizik.

KROK 1 – STANOVENÍ KONTEXTU

Krok 1 – Stanovení kontextu

Porozumění organizaci a jejímu kontextu



Vstupy:

- SWOT, PESTLE a jiné nástroje pro sběr interních a externích vlivů,
- Zkušenosti vedoucích pracovníků, strategie organizace.

Výstupy:

- Aktuální kontext organizace, včetně makroekonomických trendů,
- Zajištění návaznosti kontextu s firemní strategií.

Ukazatele (KPI's), příklady:

KPI's indikátory, příklady:

- Počet změn kontextu organizace dle nových trendů,
- Počet nově vzniklých identifikovaných a počet zaniklých rizik,
- Počet vlivů, které se nově staly kritickými či naopak ztratily na významu.

Popis aktivity:

Kontext představuje soubor vztahů, vlivů a vazeb, který musí vedení podniku brát v úvahu pro posuzování rizik v celé organizaci.

Obsahuje informace, které máme zohlednit při řízení rizik, včetně rozsahu a kritérií.

V kontextu zvažujeme:

- Interní a externí vlivy, parametry či faktory ovlivňující podnikatelské prostředí organizace,
- Potřeby a požadavky zainteresovaných stran, které se organizace rozhodla respektovat a zohledňovat při naplňování podnikatelských plánů,
- Oblasti, kterých se rizika týkají,
- Procesní řízení, umožňující řízení rizik a hodnocení efektivnosti procesů.

Kontext organizace aktualizujeme pokaždé, když dojde k významným změnám prostředí a faktorů ovlivňujících podnikání.

Monitorování a hodnocení:

Zaměřujeme se na klíčová aktiva, kterými jsou osoby zapojené do procesů organizace, nezbytné vybavení a zařízení, databáze a informační systémy, obsahující výsledky podnikání.

K tomu lze využít:

- Metodiky posuzování rizik,
- Fungující proces řízení rizik,
- Posuzování rizik při změně rozsahu systému,
- Uvědomění si změny potřeb a očekávání zainteresovaných stran (ZS),
- Zhodnocení nové ZS.

K monitorování interních vlivů můžeme využít:

- Organizační schémata s odpovědnostmi a pravomocemi vlastníků procesů,
- Zprávy týkající se ekonomiky organizace a výsledků hospodaření, zprávy o činnosti,
- Sledování záznamů z řízení výroby a poskytování služeb.

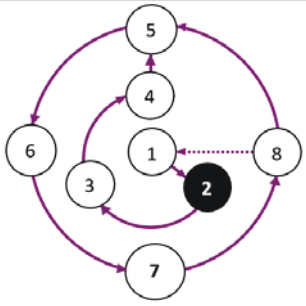
K monitorování externích vlivů lze využít:

- Podnikatelské záměry a plány,
- Podnikatelské plány a marketingové studie,
- Hodnocení zákazníky (reklamace, karta hodnocení dodavatelů – ScoreCards, loajalita),
- Mediální témata, výsledky měření prostředí, světové ceny a dostupnost zdrojů.

KROK 1 – STANOVENÍ KONTEXTU

Krok 1 – Stanovení kontextu	
Aplikace v dílčích systémech řízení	
QMS	Zohlednění faktorů v kontextu QMS umožňuje vedoucím pracovníkům řídit očekávané i neplánované změny. Kontext obvykle zahrnuje zvážení našich silných a slabých stránek, příležitostí a hrozeb (SWOT). Doporučujeme reagovat na podnikatelské, regulační, konkurenční, sociální, kulturní, finanční a politické prostředí (PESTLE), ve kterých organizace působí, a to nejen na území ČR a EU, ale i v zemích, se kterými mají vlastnické či partnerské vztahy. Příkladem výstupu je Registr interních a externích aspektů QMS.
EMS	Kontext EMS zvažuje interní a externí vlivy, související s životním prostředím včetně environmentálních podmínek jako může být dostupnost vody, kvalita ovzduší a povolování nových zdrojů, zákazy používání některých látek apod. Také tlak na uhlíkovou neutralitu či „ozelenění“ služeb a výroků patří do externích vlivů a očekávání zainteresovaných stran, které může vést až k bojkotu produktů a služeb nebo vstupů procesů. Pro dceřiné organizace jsou zásadní priority mateřské firmy, vlastníka či sponzora. Příkladem výstupu je Registr environmentálních aspektů EMS a závazných povinností.
OHSMS	Kontext OHSMS je zaměřen na plnění požadavků kladených na bezpečnost pracovníků. Tématy kontextu jsou také odvětvové požadavky (asociace, svazy, dohody, akční plány) a požadavky pracovníků (odbory, kolektivní smlouvy, rady zaměstnanců). Významně kontext OHSMS ovlivňuje míra outsourcingu, jak ve výrobě a poskytování služeb, tak v podpůrných procesech jako jsou odborně způsobilé osoby nebo pracovně lékařské služby. Příkladem výstupu je Registr potřeb a očekávání pracovníků a dalších zúčastněných stran v systému BOZP.
ISMS	Kontext ISMS zahrnuje externí a interní vlivy významné pro záměry organizace a zainteresované strany ovlivňující zejména bezpečnost informací jako jsou externí poskytovatelé ICT, poskytovatelé cloudových technologií a datových úložišť, u výrobních organizací jsou citlivá data a údaje podnikového informačního systému (ERP). Zvláštní pozornost má být věnována zpracování osobních údajů. (ISO/IEC 27001, GDPR, Zákon č. 110/2019 Sb. o zpracování osobních údajů). Příkladem výstupu je Registr informačních rizik.
BCM	Kontext BCM zahrnuje vlivy, související s udržením provozu a jsou nejvíce zranitelné při dopadu rizikových událostí na organizaci, které mohou vést až k jejímu zániku. Na rozdíl od QMS, kde se jedná především o zachování nebo zvýšení kvality dodávek produktů nebo služeb, v rámci BCM se kontext týká činností a zařízení, jejichž zničení jako následek dopadu významného incidentu (katastrofy) by mohlo vést k zániku organizace. Kontext BCM se zaměřuje na zvládnutí krizových stavů a následně na urychlené zotavení provozu po katastrofálním výpadku. Příkladem výstupu je Registr kritických aktiv.
EnMS	Kontext EnMS zvažuje energetická ohrožení provozu, týkající se odstávek a havárií energetických zařízení, související např. s preventivní údržbou či s dobou jeho fyzické životnosti pro předpovídání mezního stavu pro obnovu na základě diagnostické údržby. Příkladem výstupu je Registr významných energetických aspektů.

KROK 2 – IDENTIFIKACE RIZIK

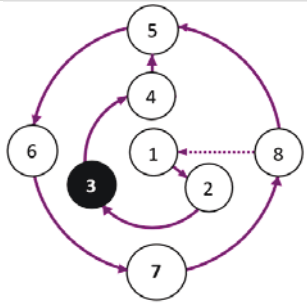
Krok 2 – Identifikace rizik Identifikace rizik na úrovni organizace a jejích procesů		
	Popis aktivity:	**Monitorování a hodnocení:**
 **Vstupy:** • Metody pro analýzu rizik pro jednotlivé procesy, • Kontext organizace, • Mapa procesů, • Místa potenciálních havárií, nežádoucích událostí a míst zranitelnosti. **Výstupy:** • Identifikované zdroje rizik, hrozeb, událostí, příčin a následků, scénáře apod., • Stanovení strategických rizik. **Ukazatele (KPI's), příklady:** KPI's indikátory, příklady: • Počet nově vzniklých rizik v procesu či vymezené oblasti, • Trend vývoje počtu rizikových událostí v oblasti informační bezpečnosti, • Míra překročení mezní hranice signálu pro vznik rizika.	Identifikace rizik představuje vymezení oblastí, ve kterých nastalo nebo může nastat riziko narušení provozu organizace, tj. procesů, systémů, informací, lidí, majetku, nasmlouvaných partnerů a dalších zdrojů, které je podporují. Identifikace rizika je klíčovým krokem v procesu řízení rizik. Musíme zajistit, že budou identifikována všechna významná rizika. Soustředíme se nejprve na kritická aktiva, zahrnující zejména ochranu pracovníků, ale i ochranu hmotných a nehmotných aktiv. Identifikace všech rizikových faktorů poskytuje lepší pochopení rizika a napomáhá při zvažování opatření k ošetření rizik. Správná identifikace rizik omezuje duplicitní rizika a upřesňuje význam rizika pro organizaci. V této fázi není nutno přihlížet k následkům.	Vedení má různé možnosti monitorování a hodnocení rizik. Příklady postojů: • Vnímání rizika – věnování pozornosti, akceptace názorů zainteresovaných stran na riziko, • Smysl pro riziko – citlivost, ochota zabývat se rizikem, zabývat se spoluúčastí, • Přijetí rizika – vědomé rozhodnutí převzít určité riziko a odpovědnost za jeho řízení, • Tolerování rizik – ochota organizace a jejích zainteresovaných stran podstupovat riziko, tj. nést dopady vyplývající z každého jednotlivého rizika po ošetření, • Nechuť zabývat se riziky – postoj spočívající v odmítání rizik, • Přenesení rizika – smluvní přenesení rizika na 3. osobu nejčastěji formou pojištění (užívá se pro rizika s nízkou pravděpodobností a významným dopadem), • Vyhnutí se riziku – vytvoření podmínek, za kterých jsou výskyt nebezpečí (hrozby) nebo zranitelnost a zasažení aktiv nepravděpodobné.

Krok 2 – Identifikace rizik	
Aplikace v dílčích systémech řízení	
QMS	Při identifikaci rizik vyhledáváme interní rizika týkající se řízení organizace, jejího provozu, aktiv a souvisejících procesů. Následně zmapujeme externí rizika, především outsourcing (kooperace), včetně externích poskytovatelů služeb. Zdroje rizik identifikujeme v celém rozsahu organizace, tj. v jednotlivých procesech jako jsou obchod, vývoj, nákup nebo výroba. Hmotná aktiva v QMS představují infrastrukturu a mohou zahrnovat budovy a související technické vybavení, ICT zařízení, včetně hardwaru nebo prostředky zajišťující transport.
EMS	Rizika EMS zahrnují negativní vlivy provozu technologických zařízení, poskytovaných produktů a služeb na životní prostředí. Zvažujeme environmentální aspekty, závazné povinnosti i další vlivy a požadavky z kontextu. Do identifikace rizik EMS je důležité zahrnout celý areál provozu, ale také dodavatelsko-odběratelský řetězec (LCA – posuzování životního cyklu), protože významným rizikem může být selhání dodávaného produktu či služby u zákazníka. Z environmentálního hlediska tedy musíme zahrnout také rozšířenou odpovědnost za výrobky nebo ekologickou újmu.
OHSMS	Nejdůležitějším aktivem OHSMS jsou lidé, systém proto musíme zabezpečit ochranu pracovníků a návštěv. Analýza rizik BOZP podléhá zákonným požadavkům, které udává § 102 odst. 3 zákona č. 262/2006 Sb. zákoník práce. Zaměstnavatel je povinen pravidelně vyhledávat nebezpečné procesy, zdroje nebezpečí nebo negativní vlivy pracovního prostředí, které mohou zapříčinit pracovní úrazy. Zdrojem rizik jsou také skoro-nehody (uniknutí o vlas) a vnášené látky, předměty, nářadí, zápůjčky dodavatelů apod.
ISMS	Snížením dostupnosti informací souvisejících s podnikáním je v řadě případů kritickým ohrožením fungování organizace. Zabýváme se zranitelností hmotných (HW) či nehmotných aktiv (SW). Zahrnout můžeme ICT, úložiště datových souborů, uživatelské dokumentace, včetně licenční ujednání k SW, autorských práv, nebo ochrany osobních údajů. Součástí identifikace nehmotných aktiv je jejich ocenění, např. nákladů na pořízení a obnovu dat a údajů v informačním systému. Identifikace hrozeb hmotných aktiv zahrnuje především výpočetní techniku, tj. pevné i přenosné počítače, mobilní telefony, prvky IoT, infrastrukturu sítí, mobilní aplikace nebo média. Zvláštní pozornost vyžaduje tzv. lidský faktor.
BCM	Identifikace rizik pro BCM vychází z tzv. BIA analýzy, což je analýza dopadů nepříznivých událostí na podnikání, které mohou vést až k zániku organizace. Zpravidla mezi ně patří ztráta aktiv, nedostupnost informací, narušení subdodávek a další negativní následky událostí a změn u zákazníků.
EnMS	Identifikaci zdrojů rizika v EnMS provádíme pomocí různých metod jako je FMEA nebo HAZOP, jednodušším způsobem je sestavení dotazníku (checklistu).

KROK 3 – ANALÝZA RIZIK

Krok 3 – Analýza rizik

Analýza rizik se zaměřuje na systematické shromažďování informací k identifikaci, popisu, odhadu a ocenění rizika



Vstupy:

- Metody pro analýzu rizik pro jednotlivé procesy z procesní mapy,
- Místa potenciálních havárií, nežádoucích událostí a míst zranitelnosti.

Výstupy:

- Určení následků a pravděpodobnost vzniku rizika,
- Matice a mapy rizik,
- Spouštěcí signály pro blížící se riziko,
- Eskalační postupy.

Ukazatele (KPI's), příklady:

KPI's indikátory, příklady:

- Maximální doba výpadku (MAO),
- Podíl aktiva na výnosech organizace,
- Náklady na opětovné pořízení aktiv a na jejich zprovoznění,
- Výše penále a pokut správních orgánů.
- Náklady na řešení škod u zákazníků.

Popis aktivity:

Analýzou rizik získáváme podklady k vyhodnocení rizik. Zahrnuje zvažování událostí (zdrojů a příčin rizik), jejich pozitivní nebo negativní dopad na organizaci.

V rámci analýzy rizik řešíme kritická aktiva organizace, posuzujeme jejich význam a určujeme jejich hodnotu.

Rozlišujeme kvalitativní a kvantitativní analýzu rizik nebo jejich kombinaci.

- Kvalitativní analýza rizik umožňuje snadno a rychle identifikovat významná rizika.
- Kvantitativní analýza používá číselného hodnocení.

Monitoring nám umožňuje sledování mezní hranice pro vznik možného odchýlení se od plánovaných výsledků (rizikových ukazatelů).

Monitorování a hodnocení:

Zaznamenávání údajů probíhá v návaznosti na vybrané ukazatele rizik.

Pro analýzy rizik máme k dispozici např.:

- Analýzu dopadů právních rizik,
- Analýzu dopadů podnikatelských rizik,
- Analýzu rizik dopadu environmentálních aspektů,
- Analýzu dopadu rizik BOZP,
- Analýzu zranitelnosti,
- Posuzování rizik při narušení kontinuity činností.

Stanovení kritérií pro blížící se riziko je klíčovou aktivitou pro monitorování ukazatelů, hodnot či údajů.

Které dostupné informace můžeme využít:

- Zákony a vyhlášky,
- Technické předpisy,
- Bezpečnostní předpisy,
- Materiálové specifikace a bezpečnostní listy,
- Technická a výkresová dokumentace.

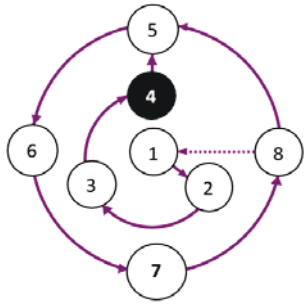
Výstupem je záznam z analýzy, katalog rizik a navržená opatření pro minimalizaci rizik, která překročila kritickou mez, tzv. Plán zvládání rizik.

Krok 3 – Analýza rizik	
Aplikace v dílčích systémech řízení	
QMS	Rozsah a podrobnost analýzy se odvíjí od složitosti organizace, např. státní instituce, zdravotní pojišťovny mají vlastní metody pro řízení rizik, nadnárodní organizace mají rovněž kaskádovitě zorganizované analýzy, které mají zpracovanou vlastní metodiku. V rámci QMS můžeme využít jednoduchý způsob provádění analýz rizik, např. SWOT analýza.
EMS	V EMS využíváme tzv. analýzy environmentálních aspektů, tedy analýzy rizik, týkající se vlivu dopadů procesů a produktů organizace na životní prostředí. Norma ISO 14001 vyžaduje další analýzy rizik související se schopností organizace plnit všechny právní požadavky na životní prostředí. Důležitým zdrojem nebezpečí ekologických havárií je větší množství nebezpečných látek skladovaných na pracovišti.
OHSMS	Norma ISO 45001 vyžaduje i analýzy rizik BOZP související se schopností organizace plnit všechny legislativou požadované aspekty, které mohou být doplněné do jednoduchých analýz organizací. Při vyhledávání zdrojů rizik se zaměřujeme přímo na pracoviště. Pomocí seznamu otázek kontrolujeme prováděné operace, popis činností a následně určujeme nebezpečí. Nepřímé metody spočívají ve vyšetřování nehod, analýze příčin pracovních úrazů nebo nemocí z povolání. Zdrojem příčin je také lidské selhání, tj. přehlédnutí nebo opomenutí použití bezpečnostních zařízení či OOPP atp.
ISMS	Úvodní etapa zavádění bezpečnosti IS v organizacích; základní fáze životního cyklu. Analýza rizik musí zahrnovat identifikaci aktiv, ocenění významnosti identifikovaných aktiv a následně provedení identifikace významných hrozeb a výše jejich dopadů na identifikovaná aktiva a posouzení pravděpodobnosti, že se hrozby a zranitelnosti vyskytnou. Výstupem je záznam z analýzy a katalog rizik, kde jednotlivé listy jsou karty jednotlivých aktiv. Správné řízení a zodpovědnost za aktiva jsou nezbytné a musí být hlavní odpovědností na všech úrovních řízení.
BCM	Analýza je vyjádření dopadů způsobených selháním nebo nedostupností důležitých aktiv (lidé, majetek). Typická analýza BIA obsahuje údaje, jak dlouho může organizace bez ohrožených činností a zařízení existovat. BIA je dobrým podkladem pro rozhodování managementu.
EnMS	V rámci systému EnMS nás především zajímají naše energie, tzn. zdroje a následně místa významného užití energie, tzn. místa kde energii významně spotřebováváme. Analýza rizik by tedy měla cílit na tyto dvě oblasti, přičemž může využít standardních metod pro identifikaci rizik. Ke sledování energetické náročnosti je pro jednotlivé stroje vhodné využít IoT.

KROK 4 – HODNOCENÍ RIZIK

Krok 4 – Hodnocení rizik

Hodnocení rizik je celkový proces stanovení míry rizika



Vstupy:

- Analýza identifikovaných rizik,
- Známá rizika narušení kritických činností,
- Kritéria velikosti dopadů a pravděpodobnosti jejich výskytu.

Výstupy:

- Kvantifikovaná rizika s akcentováním těch, které překročily hranice, jež neměly být překročeny,
- Hranice rizik, které nemají být překročeny,
- Zprávy o přehodnocení rizik a prognózování dalšího vývoje rizika.

Ukazatele (KPI's), příklady:

KPI's indikátory, příklady:

- Počet rizik, která překračují hranice,
- Počet rizik, u kterých je nebezpečí, že mohou překročit hranice,
- Dopady na organizaci (následky),
- Počet překročení hranice rizik v procesu (systému),
- Míra naplnění zákonných požadavků.

Popis aktivity:

Hodnocení rizik zahrnuje porovnání úrovně rizik se stanovenými kritérii rizik při zohlednění kontextu organizace. Na základě porovnání úrovně rizik má být zvážena potřeba řešení.

Organizace musí vyhodnocovat, která rizika spojená s narušením systému, jeho procesů a produktů, musí být ošetřena. Na základě vyhodnocení se rozhodne, zda je nezbytné další ošetření rizika.

U produktových rizik zvažte požadavky na regulaci trhu jako jsou zdravotnické prostředky nebo např. v oblasti vyhrazených technických zařízení:

- Tlakové nádoby,
- Osobní ochranné pracovní prostředky,
- Zdvihací zařízení,
- Elektrická zařízení.

Kroky hodnocení (RA):

- Určit hranice systému,
- Definovat kroky v procesu,
- Identifikovat nebezpečné události,
- Popsat způsoby řízení procesu,
- Vyhodnotit následky a pravděpodobnost jejich výskytu,
- Stanovit opatření k řešení rizik.

Monitorování a hodnocení:

V tomto kroku se vyhodnocují výsledky a dochází k výběru rizik, která mají prioritu při řešení.

Oblasti provozních rizik, které máme vzít v úvahu:

- Omezení zdrojů – nedostupnost aktiv,
- Výkonnost organizace – nedodržení kapacit, objemu dle požadavků smlouvy,
- Včasnost dodávek – nedodržení termínu dodání produktů či služeb,
- Nákladovost – nedodržení kalkulovaných nákladů.

Příklady provozních rizik, které můžeme zohlednit:

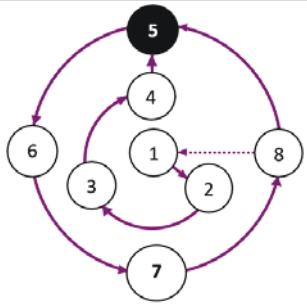
- Výstupy z revizí analýzy rizik,
- Trendy ve vývoji jednotlivých rizik,
- Revize plánů kontinuity podnikání (BCP),
- Revize plánů obnovy (RP),
- Seznam významných rizik (kritických rizik).

Krok 4 – Hodnocení rizik	
Aplikace v dílčích systémech řízení	
QMS	Vedení hodnotí míru rizika související s řízením podniku. Vyhodnocujte dopad zdrojů rizik na celopodnikové úrovni, včetně organizace a řízení. Rizika QMS se týkají následujících skupin: zákazníci (včetně uživatelů, spotřebitelů), procesy (provoz a jeho dílčí činnosti), produkty a služby (servis, návody k použití) a externí poskytovatelé (dodavatelé, kooperace).
EMS	Manažer EMS určuje významné environmentální aspekty na základě jejich environmentálních dopadů. Využívána jsou kritéria stanovená v předchozím kroku, především velikost environmentálního dopadu (zasažená plocha, doba trvání následků, chráněné druhy), aplikovatelnost či porušení závazných povinností atd.
OHSMS	Při hodnocení rizik BOZP řešte kombinace možnosti výskytu nebezpečné události (událostí) související s prací nebo expozice, a závažnosti úrazu a poškození zdraví, které mohou být způsobeny touto událostí (událostmi) nebo expozicí (expozicemi). Pro hodnocení identifikovaných rizik BOZP zapojte bezpečnostního technika, tj. odborně způsobilé osoby v prevenci rizik (OZO). Rizika máte ohodnotit pro každou specifikovanou činnost.
ISMS	Výstupem je záznam z analýzy a katalog rizik, kde jednotlivé listy jsou karty jednotlivých aktiv a navržená opatření pro minimalizaci rizik, která překročila kritickou mez, tzv. Plán zvládání rizik. Záznam z analýzy nabízí vyhodnocená rizika, určená k rozhodnutí, o prioritách potřebných opatření pro snížení rizik. Při aktualizacích analýzy rizik jsou brány v úvahu následující skutečnosti: účinnost dříve realizovaných opatření; aktuální i plánované změny, a to jak uvnitř organizace, tak i v jejím okolí (legislativa, konkurence); četnost výskytu vybraných typů bezpečnostních incidentů (aktualizace pravděpodobnosti výskytu hrozby). Při hodnocení rizik se vychází z analýzy a rizika se podle výsledku setřídí do několika stupňů kritičnosti. U nejvyššího stupně byla překročena stanovená mez a je potřeba nastavit okamžité opatření k jejich eliminaci. Střední stupeň představuje významná rizika, která jsou řízena a lze je po určitou dobu akceptovat. K rizikům nejnižšího stupně není nutné přijímat zásadní opatření.
BCM	V systému BCM stanovte priority havarijních situací. Současně vyčleňte zdroje pro řešení rizika dle závažnosti, srovnání výsledků analýzy s kritérii rizik a rozhodnutí o přijatelnosti. To může být dobrým podkladem pro vypracování havarijních plánů, ve kterých stanovíte postupy zabraňující riziku nebo zmírňující výskyt rizika.
EnMS	Vzhledem k tomu, že energie podstatným způsobem ovlivňuje výrobu či poskytování služeb, lze hodnocení rizik přímo spojit s finančními ztrátami v případě nevyrábění či neposkytování služeb. Rizika spojená se ztrátou klienta, trhu apod. jsou již sekundárními následky výše popsaného stavu.

KROK 5 – OŠETŘENÍ RIZIK

Krok 5 – Ošetření rizik

Ošetření rizik umožňuje individuální řešení rizikových situací



Vstupy:

- Výstupy z hodnocení rizik,
- Kritéria pro hodnocení,
- Výběr rizik, pro která je nutno provést ošetření pro jejich eliminaci nebo snížení.

Výstupy:

- Plány zvládání rizik,
- Projekty pro snížení rizika (opatření),
- Havarijní (nouzové) plány,
- Plány obnovy,
- Plány pro stahování produktu z oběhu,
- Odstranění (eliminace) rizika.

Ukazatele (KPI's), příklady:

KPI's indikátory, příklady:

- Podíl jednotlivých typů ošetření rizik dle hierarchie,
- Dosažení milníků projektů,
- KPI's jednotlivých procesů,
- Vývoj úrazovosti,
- Průběh vývoje incidentů.

Popis aktivity:

Výběr nejvhodnějších možností ošetření rizik zahrnuje hledání vyváženého kompromisu mezi náklady, úsilím při implementaci v porovnání k přínosům s ohledem na požadavky zákonů a předpisů a další požadavky, jako např. sociální odpovědnost a ochrana životního prostředí.

Přijměte opatření k efektivnímu pokrytí největších rizik tak, aby se účinek nejistoty snížil, resp. aby bylo eliminováno nebezpečí.

Využívejte FMEA jako prevenci procesních rizik:

- D-FMEA – opatření zejména ke snížení významnosti a/nebo pravděpodobnosti výskytu vady návrhu,
- P-FMEA – opatření zejména ke snížení pravděpodobnosti výskytu a zlepšení odhalitelnosti vady procesu.

Připravte Plány zvládání rizik, přímo navazující na analýzu a vyhodnocení rizik.

Monitorování a hodnocení:

Co můžete zvolit pro ošetření rizika:

- Snižování rizika – omezení negativních dopadů rizika (defenzivní přístupy),
- Eliminace rizika – omezení příčin vzniku rizika (prevence rizika, ofenzivní přístupy),
- Přenos rizika, tj. jeho sdílení s jinými subjekty (zákazníkem, dodavatelem, pojišťovnou apod.),
- Zbytkové riziko – snížené riziko po realizaci možných opatření na snížení rizika (řeší návod na použití produktu),
- Neošetřené riziko – náklady na opatření nejsou úměrné dopadu na organizaci.

Postupy a záznamy:

- Monitorování KPI's procesů,
- Monitorování plnění cílů,
- Dosahování milníků v rámci projektů,
- Evidence havárií,
- Evidence bezpečnostních incidentů,
- Evidence úrazů,
- Vyhodnocení plánů obnovy,
- Vyhodnocení plnění havarijních plánů.

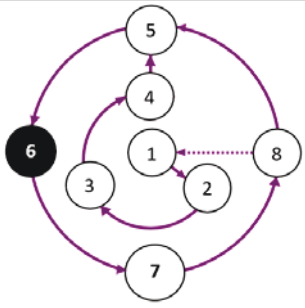
KROK 5 – OŠETŘENÍ RIZIK

Krok 5 – Ošetření rizik	
Aplikace v dílčích systémech řízení	
QMS	Při ošetření rizik si sami stanovíte přijatelnou mez, tj. tolerovanou míru rizika, a to na základě přístupu zvoleného k ošetření rizika. Ošetření rizik může probíhat po různých liniích: stanovení cílů, řízení procesů, inovační projekty, Plány zvládání rizik, nápravná opatření.
EMS	Plánováním opatření EMS zmírňujete rizika či zabraňujete nežádoucím účinkům. Neopomeňte významné environmentální aspekty a možnost, že externí podmínky životního prostředí ovlivní organizaci. Aplikujte prevenci znečišťování, která preferuje typy ošetření rizik výše v hierarchii (úplné předejití problému je výše než ošetření vzniklých následků).
OHSMS	Plánováním opatření k řešení rizik OHSMS máte zabránit nežádoucímu vzniku úrazů a nemocí z povolání. Aplikujte důsledně hierarchii způsobů řízení požadované právními předpisy i normou ISO 45001.
busi	Rizika jsou ošetřena Plánem zvládání rizik. U významných projektových rizik přijímáme opatření ke zbytkovému riziku. Tato opatření jsou zapsána do evidence Opatření ISŘ a dále podléhají procesu řízení opatření. Vývoj hodnot rizik jednotlivých aktiv umožňuje vyhodnotit účinnost jednotlivých opatření z Plánu zvládání rizik.
BCM	Efektivně řízený BCMS má v prvé fázi jednoznačně definovat odpovědnost, kompetence a komunikační postupy v případě krizové situace a mít k dispozici havarijní plány zajišťující evakuaci lidí, kontaktování kompetentních institucí, zastavení destrukce a vyhodnocení situace. Ve druhé fázi se přechází na navázání kontinuity činností aspoň prozatímním způsobem pro zajištění dodávky klientům (např. prioritním zákazníkům). Třetí fáze se týká obnovy kontinuity podnikání, což je ta část krizového managementu, která má sloužit k rychlému obnovení základních funkcí. Jeho součástí jsou tzv. plány obnovy.
EnMS	Rizika můžeme ošetřit na několika úrovních: 1. Zajištění náhradního zdroje energie, 2. Údržba a servis, 3. Monitorování a měření energií, 4. Vzdělávání a tréninku.

KROK 6 – KOMUNIKACE A KONZULTACE

Krok 6 – Komunikace a konzultace

Dialog vlastníků procesů s významnými zainteresovanými stranami



Vstupy:

- Definování rolí či pozic vlastníků rizik, manažerů rizik a dalších odpovědných osob organizace.

Výstupy:

- Nastavený proces komunikace,
- Nastavený postup pro řízení rizik,
- Nastaveny pravomoci v rámci eskalačních procedur,
- Stanoveny odpovědnosti při přehodnocení rizik po vzniku odchylky dle plánu (rizika).

Ukazatele (KPI's), příklady:

KPI's indikátory, příklady:

- Minimum správních řízení ze strany dozorových orgánů v organizaci,
- Negativní dopady na organizaci (škody na infrastruktuře, pokuty/rok),
- Počet změn v organizační struktuře/rok.

Popis aktivity:

Je na vás, zda zvažujete svá rizika intuitivně nebo s použitím metod. Všichni pracovníci s rozhodovací pravomocí mají předvídat, umět zvolit a zvládat vhodné přístupy k omezení nebo vyloučení rizik.

Vlastníci procesů jsou odpovědni za řízení rizik na úrovni procesů, mají konzultovat přístupy k posouzení a ošetření rizik s vedením organizace, ale také se zaměstnanci, kteří jsou v daných procesech zapojeni.

Externí komunikace a konzultace zaměřte na informování pro vás důležitých zúčastněných stran.

Máte mít jasno:

- Jaký přístup organizace zvolila pro řízení rizik,
- Jak monitorujeme a vyhodnocujeme rizika ovlivňující podnikání,
- Jak bude organizace zajišťovat součinnost a získávat zpětnou vazbu.

Interní konzultace využijte ke sdělování pracovníkům:

- Jakým způsobem jsou rizika řízena,
- Která klíčová rizika jsou v jednotlivých procesech,
- Kdo je odpovědný za řízení rizik.

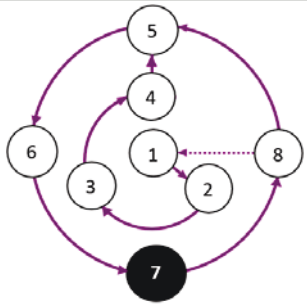
Monitorování a hodnocení:

Postupy a záznamy:

- Záznamy z porad vedení,
- Komunikace se zainteresovanými stranami,
- Zprávy z interních auditů systému,
- Hodnocení prověrek (BOZP),
- Hodnocení souladu s právními požadavky,
- Zpráva o přezkoumání systému managementu,
- Zprávy o přehodnocení rizik a prognózování vývoje rizika,
- Software pro řízení rizik,
- Procesní mapy s pozicemi či rolemi manažerů rizik a odpovědnostmi a pravomocemi pro alternativní řízení procesů.

Krok 6 – Komunikace a konzultace	
Aplikace v dílčích systémech řízení	
QMS	Zaměřujeme se na nastavení rolí či pozic pro fáze stanovení rizik a následné řízení rizik. Vhodné je definování zodpovědností a pravomocí mezi vlastníky procesů a odborníky na řízení rizik, kteří vstupují do procesu řízení rizik. V rámci systému mají být stanoveny způsoby komunikace při řízení rizik. Důležité je dodržování zákonných požadavků, respektování požadavků technických předpisů a interních postupů.
EMS	Zdrojem informací pro komunikaci a konzultace o rizicích jsou registry (environmentálních aspektů, závazných povinností apod.), ale zejména havarijní plány. Významným prvkem jsou výstražné symboly a značky. Do komunikace při managementu rizik patří stanovování cílů, vyhodnocování jejich plnění, což je pravidelný reporting na všech úrovních (výsledků manažerských i provozních procesů), týkajících se environmentální výkonnosti. Zvažte nouzové způsoby komunikace v případě mimořádných událostí.
OHSMS	Školení, osvěta, výstrahy, značení, ale i intranet, nástěnky a dokumentace. U OHSMS vyžadujte dodržování právních předpisů a jiných požadavků, představujících plnění dohod s pracovníky (např. kolektivní smlouva) nebo dokumenty předepisující zajištění ochrany a zdraví pracovníků (např. hygienické předpisy, pravidla pro nakládání s chemickými látkami).
ISMS	Stanovte shodu s právními požadavky a smluvními závazky (např. dodržování licencí a autorských práv). Výhodou jsou dobře zpracované interní postupy pro dodržování pravidel ISMS. Proškolujte pracovníky ve vztahu k dodržování pravidel ISMS, vyhlášek Kybernetického zákona, aby byla stanovena shoda s právními požadavky a smluvními závazky (např. dodržování licencí a autorských práv). Zaznamenávejte a vyhodnocujte informačních incidenty, využijte a trendy vývoje těchto incidentů k získání obrazu o řízení informačních rizik. Provádějte předepsané testy plánů obnovy na klíčových zařízeních IT a zaznamenávejte výsledky. Získáte důkazy o zárukách udržitelnosti chodu IT po předepsané období, které bývá součástí smluv se zainteresovanými stranami.
BCM	Provádí se dvoufázově. Vyžadujte dodržování programu Havarijních opatření v první fázi řešení důsledků havárie a následně dodržování technických a organizačních předpisů souvisejících s technologiemi na podporu obnovy infrastruktury po výpadku či přerušení provozu v rámci druhé fáze řešení důsledků havárie. Nedílnou součástí BCM je provádění nácviku a prověřování postupů pro případ obnovy infrastruktury.
EnMS	V systému EnMS máme mít nastaveny způsoby komunikace pro sledování a sběr dat externími poskytovateli (fakturační měřidla), které typicky monitorují elektřinu, zemní plyn, nakupované teplo, případně i pohonné hmoty. Dále je žádoucí sledovat spotřebu užitkové i pitné vody.

KROK 7 – MONITOROVÁNÍ A PŘEZKOUMÁNÍ

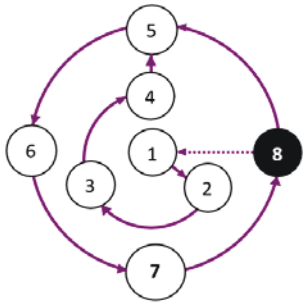
Krok 7 – Monitorování a přezkoumání Udržování a aktualizace systémů managementu, zpětná vazba vedení		
	Popis aktivity:	**Monitorování a hodnocení:**
 **Vstupy:** • Plány kontinuity • Programy řízení kontinuity • KRI's – Klíčové ukazatele prevence rizik • Mezní signální hranice pro vznik rizik **Výstupy:** • Revize analýzy rizik • Nastavení frekvence přehodnocení ukazatelů rizik • Měření výkonnosti systému řízení rizik v procesech • Periodické přezkoumání systému řízení **Ukazatele (KPI's), příklady:** KPI's indikátory, příklady: • Udržitelnost podnikání v přijatelném tolerančním rozsahu hlavní činnosti, • Přesnější plánování výkonů, • Výkonnost systému řízení rizik, • Četnost změn v systému řízení rizik, • Četnost zpětných vazeb od vlastníků procesů o nefunkčnosti systému, • Analýza trendů vztažená k ukazatelům KPI's/KRI's.	Organizace je vystavena změnám prostředí, na které musí vhodně reagovat. Pro zajištění aktuálnosti se vyžaduje pravidelné monitorování a přezkoumání. Jsou-li informace o riziku nepřesné, můžeme učinit nesprávná rozhodnutí, která by jinak mohla být vyloučena. Do přezkoumání zahrnujeme vyhodnocení příčin: • Přerušení provozu, • Havárií, • Rizikových stavů bezpečnostních incidentů, • Skoro-nehod a pracovních úrazů, • Informačních událostí a incidentů, • Incidentů v rámci poskytování služeb, • Incidentů způsobených změnami, • Zjištění z auditů a kontrol. Aktualizace ukazatelů pro výkonnost systému řízení rizik, příklady: • Změny požadavků na environmentální výkonnosti procesů, • Aktualizace požadavků na výkonnost systému managementu BOZP.	Cílem je prověřit správnost nastavení systému řízení rizik. Na výstupu je fungující systém či proces řízení rizik, který organizaci přináší výsledek ve formě prevence před pokutami či negativními dopady. Pozitivním dopadem může být také zlepšení vztahů mezi zúčastněnými stranami. Provádějte pravidelnou kontrolu a aktualizujte obchodní či výrobní plány umožňující odhadovat ztráty. Podávejte hlášení a veďte záznamy o výsledcích řízení rizik, příklady: • Opakované hodnocení plánů kontinuity (BCP), • Aktualizace pojistných smluv, • Poučení z havarijních situací a incidentů, • Zprávy o přehodnocení rizik a prognózování vývoje rizika.

Krok 7 – Monitorování a přezkoumání	
Typické KPI's v dílčích systémech řízení	
QMS	• Plnění strategických cílů, • Plnění ročních cílů, • Dosahování cílových hodnot KPI v rámci procesů, • Trendy úspěšnosti dodavatelů, • Úspěšnost v rámci projektů.
EMS	• Vývoj znečištění vypouštěných vod, • Vývoj emisí, • Vývoj spotřeby chemických látek, • Vývoj v množství (nebezpečných) odpadů, • Plnění cílů environmentální výkonnosti, • Míra plnění zákonných požadavků, • Vývoj v počtu stížností z okolního prostředí, • Vývoj kritických zjištění od kontrolních orgánů.
OHSMS	• Plnění cílů s ohledem na bezpečnost prostředí, • Míra plnění zákonných požadavků, • Vývoj v počtu úrazů, • Vývoj kritických zjištění od kontrolních orgánů, • Vývoj v povědomí zaměstnanců.
ISMS	• Plnění strategických cílů, • Plnění operativních ročních cílů, • Trendy výkonnosti IT technologií (dostupnost, důvěrnost, integrita), • Trendy výkonnosti dodavatelů (dostupnost, důvěrnost, integrita), • Trendy při implementaci informační bezpečnosti, • Vývoj reálných nákladů pro nejhorší dopad neošetřených bezpečnostních rizik, • Podíl bezpečnostních incidentů.
BCM	• Pochopení rizik, ohrožujících udržitelnost podnikání, • Identifikování potenciálních dopadů přerušení dílčích procesů, • Rozšíření povědomí i kompetencí personálu, • Zvýšení důvěryhodnosti organizace a jejího podnikání, • Získání konkurenčních výhod, • Doba cyklu pro obnovení činnosti.
EnMS	• Vývoj ve spotřebě paliv, • Vývoj ve spotřebě elektrické energie, • Monitorování poruch a jejich příčin, • Ztráty v distribučních sítích, • Ztráty v tlakových potrubích.

KROK 8 – UDRŽITELNOST PODNIKÁNÍ

Krok 8 – Udržitelnost podnikání

Zajištění kontinuálního dosahování kritických cílů v organizaci



Vstupy:

- Analýza BIA,
- Havarijní plány,
- Plány obnovy,
- Plány kontinuity podnikání.

Výstupy:

- Optimální chod organizace v havarijních či krizových situacích,
- Vhodná opatření k nasazení bezprostředně po výpadku.

Ukazatele (KPI's), příklady:

KPI's indikátory, příklady:

- Doba cyklu obnovení činnosti,
- Maximálně akceptovatelný výpadek (MAO),
- Maximálně přípustná doba narušení (MTPD),
- Cílová doba zotavení (RTO),
- Cílový bod zotavení (RPO),
- Počet stahování produktů z trhu.

Popis aktivity:

Udržitelné podnikání představuje způsobilost organizace trvale dodávat produkty nebo služby na přijatelné, předem definované úrovni v nebezpečných situacích či po narušení provozu.

Management má mít pod kontrolou a řídit nežádoucí události.

Řízení incidentů představuje činnosti prováděné na místě události.

Zajistěte provoz a procesy zavedením krizového řízení, které umožní bezprostřední reakci na havárie, a určete spouštěcí signály pro nasazení havarijních plánů.

Řízení kontinuity představuje zajištění provozu a procesů, aby se po přerušení mohly co nejdříve vrátit do původního stavu:

- Použijte plány krizového řízení. Zajistěte udržení klíčových procesů a chod hlavních podnikatelských aktivit,
- Při identifikace kritických procesů vycházejte z přezkoumání strategických plánů a určování kritických faktorů úspěchu,
- Neopomíjejte externí rizika – dodavatele, kooperace, outsourcing.

Monitorování a hodnocení:

Do přezkoumání zapojte vlastníky procesů a navazující funkce, které jsou odpovědné za splnění cílů a souvisejících ukazatelů.

Strategické scénáře mohou zvažovat:

- Zamezení přístupu do prostor např. v případě hrozby bombového útoku,
- Absenci pracovníků např. virové pandemie,
- Selhání technologií a podpůrných zařízení,
- Selhání klíčového poskytovatele služeb.

Jejich součástí jsou definované úlohy lidí a týmů, které přejímají pravomoci v případě havárií a bezprostředně po ní, podrobnosti, jak komunikovat uvnitř i vně organizace, a to včetně komunikačních kanálů pro bezprostřední záchranu především lidí a zabránění dalších ztrát vybavení pro podnikání.

Úspěšně zvládnutá negativní událost může významně zvýšit důvěru zákazníků.

Krok 8 – Udržitelnost podnikání	
Aplikace v dílčích systémech řízení	
QMS	Systémy managementu kvality vyžadují způsobilost organizace trvale dodávat produkty nebo služby na přijatelné, předem definované úrovni v nebezpečných situacích či po rušivém incidentu. Konkrétními příklady řešení nouzových situací jsou havarijní plány v automobilovém průmyslu nebo plány stahování závadných produktů z trhu v potravinářství.
EMS	U EMS se jedná o vypracování havarijních plánů, reagujících např. na potenciální ekologickou újmu, výkyvy počasí i podnebí. Zákonem jsou stanoveny podmínky, za nichž vzniká podnikatelům a dalším osobám vykonávajícím rizikovou provozní činnost povinnost provádět preventivní a v případě vzniku ekologické újmy povinnost provádět nápravná opatření.
OHSMS	Po závažných haváriích, nehodách či úrazech a poškození zdraví zajistěte v souladu s plány první pomoci komunikaci se složkami státní správy, neopomeňte o zdravotním stavu pracovníků informovat jejich rodinné příslušníky.
ISMS	Práce s informacemi se dnes provádí především prostřednictvím stále se vyvíjejících IT technologií představující nové hrozby např. mobilní aplikace. V ISMS se management kontinuity týká především včasné obnovy ICT. Obnova IT infrastruktury po bezpečnostním incidentu představuje příklad plánování obnovy (RP) pro další oblasti. Ukázka jednoduchého plánu. Příklady měření výkonnosti: RTO, RPO.
BCM	Pomocí plánů kontinuity budete reagovat na narušení, použijete postupy pro následné zotavení a znovu zahájení provozu na předem definovanou úroveň. Vyhodnocujte výkonnostní ukazatele, které napomohou ke zlepšování systému. Příklady ukazatelů: MAO, MTPD.
EnMS	Havarijní plány zaměřte především na zajištění stabilního zdroje energie a následně na efektivní využití této energie pro strategické procesy, které zajistí výrobu či poskytnutí služby nebo bezpečného odstaveni zařízení, tak aby nedošlo ještě k větším ztrátám či ohrožení.

Publikaci připravila Sekce kvality HK ČR, na projektu se podílel kolektiv autorů: Ing. Milan Trčka, vedoucí projektu, výkonný ředitel NQA CZ s.r.o.; Ing. Jan Svobodník, EurChem, výkonný ředitel QUALIFORM, a.s., Ing. Jana Olšanská, výkonný ředitel CQS, vedoucí certifikačního orgánu CQS a Ing. Marie Šebestová, auditorka, CQS – Sdružení pro certifikaci systémů jakosti, Ing. Petr Houdek, poradce HCOMP Praha, s.r.o., Mgr. Miroslav Krčma, poradce IRCON, s.r.o. a Ing. Jiří Vích MBA, jednatel Komora s.r.o. Odbornou korekturu provedla Ing. Lucie Hrbáčková, akademický pracovník, Fakulta managementu a ekonomiky, Univerzita Tomáše Bati ve Zlíně.

Sekce kvality Hospodářské komory České republiky

Hlavním cílem Sekce kvality HK ČR je iniciovat a podporovat aktivity, které vedou ke zlepšování podnikatelského prostředí, úspěšnosti a výkonnosti v podnikání a k růstu konkurenceschopnosti podnikatelských subjektů na trhu ČR i v zahraničí.

Sekce kvality HK ČR má 5 pracovních skupin, viz struktura Sekce na www. komora.cz, s cílem naplňovat Strategii národní politiky kvality ČR a Strategii HK ČR v oblasti kvality.

Zaměření pracovních skupin:

- Pracovní skupina 1 – Pravidla praxe, osvědčování kvality podnikání, cena kvalitní služby, celoživotní vzdělávání, technické normy, znalectví.
- Pracovní skupina 2 – Kvalita podnikání a profesí ve vztahu k výkonu těchto profesí (systémy řízení, zlepšování výkonnosti), ve vztahu k infrastruktuře kvality a ve vztahu ke spotřebiteli, kvalita certifikace (zákaznická vazba).
- Pracovní skupina 3 – Společenská odpovědnost organizací a udržitelný rozvoj, cena „Podnikáme odpovědně“ NPK.
- Pracovní skupina 4 – Kvalita ve veřejných zakázkách, kvalitativní hodnotící kritéria v EU projektech – aplikace v ČR, bezpečnost stanovených výrobků v provozu.
- Pracovní skupina 5 – Kvalita certifikace, zákaznická vazba.

Sekce kvality HK ČR je otevřenou sekcí a spolupracuje s Českou společností pro jakost, dalšími Sekcemi HK ČR, Odbornými sekcemi Rady kvality ČR, Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví, Českou agenturou pro standardizaci, Ministerstvem průmyslu a obchodu a dalšími ministerstvy, Českým institutem pro akreditaci, a dalšími partnery (viz složení Sekce na webu).

Vydala v říjnu 2020 Hospodářská komora České republiky
Florentinum, Na Florenci 2116/15
110 00 Praha 1

www.komora.cz

Tel.: +420 266 721 300
E-mail: office@komora.cz