

„Požiadavky na riadenie rizík a príležitostí z
pohľadu aktuálnych certifikačných noriem,
skúsenosti z praktického výkonu auditov
nových požiadaviek ISO noriem na riadenie
rizík z pohľadu audítora systémov
manažérstva“

Ing. Pavel Horník, TÜV SÜD Slovakia

eFOCUS



Slovakia

- **Predstavenie** prednášajúceho
- **Úvod do témy** - manažérske systémy a riziká
- **Požiadavky na riadenie rizík a príležitostí**
 - z pohľadu aktuálnych certifikačných noriem
- **Skúsenosti z praktického výkonu auditov nových požiadaviek ISO noriem na riadenie rizík**
 - z pohľadu audítora systémov manažérstva
- **Otázky**
- **Záver**

Predstavenie prednášajúceho

Ing. Pavel Horník

25 rokov praktického výkonu v oblasti certifikácie a školení

Celkovo vykonaných viac ako 1600 certifikačných auditov v rôznych systémoch

Vedúci audítor pre akreditované certifikačné schémy:

ISO 9001 - Manažérstvo kvality; ISO 14001 - Environmentálne manažérstvo

ISO /OHSAS 18001 - Ochrana a bezpečnosť zdravia pri práci

ISO/TS 16949, VDA 6.1 - Systémy manažérstva kvality pre dodávateľov do AP

ISO 50001 - Energetické manažérstvo

ISO/IEC 27001 - Manažérstvo informačnej bezpečnosti

ISO/IEC 20000 - 1 - Manažérstvo poskytovania IT služieb

eIDAS - Kvalifikovaná dôveryhodná služba validácie kvalifikovaných
elektronických podpisov , pečatí

ISO/IEC 22301- Systém riadenia kontinuity podnikania - neakreditované;

ISO/IEC 27018 - Ochrana osobných údajov v Cloude – neakreditované



„Všetka ekonomická činnosť je svojou povahou vysoko riziková.“

Peter Ferdinand Drucker

(Rakúšan Peter Ferdinand Drucker je pokladaný za zakladateľa moderného manažérstva ako samostatného teoretického odboru. Je autorom celého radu teórií a inovatívnych konceptov v oblasti manažérstva – napr. Diskontinuita, Manažérske funkcie / činnosti, Sedem nových úloh manažéra budúcnosti, Účel, funkcia a zámery podniku, Poznanie a riadenie rizík,)

Kedže normy pre manažérske systémy pracujú už s týmito pojmami k rizikám ako „s hotovou vecou“, niečo krátke na úvod :

Riadenie rizík (Risk Management) je oblasť riadenia - zameriavajúca sa na analýzu a zníženie rizika, pomocou rozličných metód a techník prevencie rizík, ktoré eliminujú existujúce alebo odhaľujú budúce faktory zvyšujúce riziko. Riziko je všade prítomným a charakteristickým sprievodným javom fungovania organizácií v súčasnom turbulentnom podnikateľskom prostredí.

Prakticky :

Riadenie rizík je sústavná, opakujúca sa množina navzájom previazaných aktivít, ktorých cieľom je riadiť potenciálne riziká, teda obmedziť pravdepodobnosť ich výskytu alebo znížiť ich vplyv.

Účelom riadenia rizík je predísť problémom či negatívnym javom, zamedziť vzniku problémov a tak sa vyhnúť neštandardným situáciám - **krízovému riadeniu**.

Riadenie rizík sa skladá zo štyroch vzájomne previazaných fáz, a to z **identifikácie rizík**, **hodnotenia rizík**, **zvládnutia rizík** (respektíve ich **zmiernenia**) a **monitoringu rizík**.

Riziká – čo tam vlastne možno zaradiť ?

- **Ekonomické a finančné riziká** (napr. úverové riziká, Investičné riziká (odhad ziskovosti a návratnosti investície), poisťovacie a zaistovacie riziká (napr. odhad veľkosti rizika a pravdepodobnosti poistnej udalosti).....
- **Projektové riziká** (napr. zlé riadenie projektov, nezvládnutie zmien, ...)
- **Trhové riziká** (napr. riziká spojené s úspešnosťou podniku na trhu, dopytové a predajné riziká, riziká spojené s preferenciami spotrebiteľov, správaním sa konkurencie,...).
- **Technické riziká** (napr. technologické, inovačné - spôsobené použitím nových alebo nevyskúšaných technológií, technických zariadení, materiálov či výrobných prostriedkov. Technické riziká existujú vďaka neustálemu rozvoju a inováciám a vznikajú v dôsledku zavádzania nových produktov na trh,...)

Riziká – čo tam vlastne zaradiť ? (2)

- **Sociálne riziká** (napr. spojené so správaním sa a konaním ľudí, možno sem zaradiť manažérske riziká (napr. riziká spojené s nevhodnými rozhodnutiami manažérov a vlastníkov firiem), sociálno - patologické riziká (napr. podvody, krádeže,...), skupinové hrozby (napr. masová migrácia z miest so zlou hospodárskou situáciou, prírodnými katastrofami, rôznymi konfliktami), zdravotné riziká (napr. riziko pandémie),.....
- **Prevádzkové riziká** (napr. riziká vyplývajúce z výpadku plynulej prevádzky alebo poruchy (výpadky elektrickej energie, siete, poruchy a havárie - kvôli ktorým sú vyrobené nepodarky alebo zastavená výroba), náhrada za chorého pracovníka alebo pracovníka odchádzajúceho z pracovného miesta

Riziká – čo tam vlastne zaradiť ? (3)

- **Bezpečnostné riziká (Security Risks)**

Personálna bezpečnosť (napr. poškodenie majetku, zdravia a života osôb, ochrana osobných údajov),

Fyzická bezpečnosť (napr. poškodenie zariadenia, narušenie objektov a systémov),....

Informačné riziká (napr. narušenie bezpečnosti siete, informačného systému, zneužitie alebo poškodenie dát,.....

- **A ďalšie.....**

Riziká – ako sa k nim dopracovať ?

- Zásadná pre riadenie rizík - je ich analýza. Pomocou **analýzy rizík** sa zisťuje miera nebezpečenstva, ktorému je firma vystavená – tiež známa pod pojmom **hrozba**

(- pre označenie zdroja akejkoľvek negatívnej udalosti, sily, osoby alebo aktivity, ktorá chce - alebo môže poškodiť nejakú hodnotu. Niekedy sa tiež používa pojem nebezpečenstvo. Hrozba má nežiaduci vplyv na bezpečnosť alebo môže spôsobiť škodu, stratu, nežiaduce zmenu, či iný nežiaduci jav).

Riziká – ako sa k nim dopracovať ? (2)

- ako veľmi sú jej aktíva

(pojem, ktorý označuje **majetok** firmy či hospodárske prostriedky. Pod pojmom majetok rozumieme súhrn všetkých vecí, osôb, peňazí, pohľadávok a iných majetkových hodnôt, ktoré patria **vlastníkovi** a slúžia k **podnikaniu**. Aktíva sú prostriedky kontrolované firmou, u ktorých sa predpokladá, že nejakým riadeným spôsobom prinesú vlastníkovi budúci ekonomický úžitok).....

Riziká – ako sa k nim dopracovať ? (3)

- týmito hrozbami **zraniteľné** !!!

(zraniteľnosť - pojem, je pojem používaný v riadení rizík pre označenie slabiny či nedostatku vo vzťahu k aktívu. Zraniteľnosť umožňuje uplatnenie /dopad hrozby. Pri **analýze rizík** je zraniteľnosť vlastnosťou aktíva. Zraniteľnosť je charakterizovaná predovšetkým pomocou dvoch faktorov:

Citlivosť (náchylnosť k spôsobeniu rizika uplatnenou hrozbou)

Kritickosť (význam aktíva pre firmu, jednotlivca či systém)

Využitie zraniteľnosti v praxi: Zraniteľnosť spoločne s hrozbou slúži na posúdenie veľkosti a pravdepodobnosti naplnenia rizika. Pri porovnateľnej úrovni hrozby vedie nižšia miera zraniteľnosti k nižšej miere rizika - a opačne).

Riziká – ako ich analyzovať, riadiť?

Medzi najznámejšie metódy a metodiky v oblasti riadenia rizík patrí:

- Basel I - III - pravidlá kapitálovej primeranosti týkajúce sa prevádzkových rizík bánk
- CorIA (Core Impact Assessment)
- CLA (Checklist analysis) - analýza kontrolným zoznamom
- CCA (Cause-Consequence Analysis) - analýza príčin a následkov - kombinácia FTA a ETA
- **CRAMM** (CCTA Risk Analysis and Management Method) - analýza rizík a riadenie bezpečnosti informácií
- CPQRA (Chemical Process Quantitative Risk Analysis) - kvantitatívne hodnotenie rizika chemického procesu

Riziká – ako ich analyzovať, riadiť? (2)

Medzi najznámejšie metódy a metodiky v oblasti riadenia rizík patrí:

- EWRM (Enterprise-Wide Risk Management)
- **ETA** (Event tree analysis) - analýza stromu udalostí
- **FMEA** (Failure Modes and Effects Analysis) - analýza možných chýb a ich následkov
- FMECA (Failure Mode, Effects and Critically Analysis) - analýza možných chýb a ich kritických následkov
- **FTA** (Fault Tree Analysis) - analýza stromu poruchových stavov
- HAZOP (Hazard and Operability Study) - riziková a operačná analýza

Riziká – ako ich analyzovať, riadiť? (3)

Medzi najznámejšie metódy a metodiky v oblasti riadenia rizík patrí:

- HAZID (Hazard Identification Study) - štúdie identifikácia nebezpečenstva
- HRA (Human Reliability Analysis) - analýza ľudskej spoľahlivosti
- Kognitívne modelovacie štruktúry pri identifikácii a hodnotení rizík
- PHA (Preliminary Hazard Analysis)
- PPAP (Production Part Approval Process)
- **5 WHY?** (5 krát prečo?)

Riziká – ako ich analyzovať, riadiť? (4)

Medzi najznámejšie metódy a metodiky v oblasti riadenia rizík patrí:

- Prognózovanie
- Pravdepodobnostné metódy
- RIPRAN (Risk Project Analysis)
- RR (Relative ranking) - relatívna klasifikácia
- SA (Safety Audit) - bezpečnostný audit
- SR (Safety Review) - bezpečnostná prehliadka
- VaR (Value at Risk)
- WI (What-if Analysis) - Čo keď ... analýza
- Winterlingova krízová matica

Riziká – ako ich analyzovať, riadiť? (5)

Medzi najznámejšie analytické techniky použiteľné pre identifikáciu potenciálnych rizík v oblasti riadenia rizík patrí:

- RMF (Risk Management Framework) - National Institute of Standard and Technology EN
- M_o_R (Management of Risk)
- **RiskIT** (Risk IT Framework, ISACA)

Riziká – ako ich analyzovať, riadiť? (6)

Medzi najznámejšie nástroje a techniky použiteľné pre tímovú prácu v oblasti riadenia rizík patrí:

- **Brainstorming, Brainwriting**
- Analýza 5F (Five Forces)
- PESTLE analýza
- **SWOT** analýza
- VRIO analýza
- **Paretovo pravidlo (analýza)**
- Prognózovanie
- **SMART** - návrh cieľov
- Technika scenárov

Riziká – ako ich analyzovať, riadiť? (7)

- S pojmom riziko súvisí pojem „**neistota**“, ktorý znamená možnosť rôznych výsledkov, ktorých pravdepodobnosť nie je kvantifikovaná.
- **Najdôležitejšími charakteristikami rizika sú:**
- **Miera pravdepodobnosti rizika** - pravdepodobnosť, že riziko nastane
- **Úroveň rizika**
- **Vplyvy rizika** - dôsledky, ktoré sa prejavujú, ak nastane riziková situácia
- **Predvídateľnosť riziká** - šanca, že riziko je možné vopred identifikovať a predvídať

Riziká – ako ich analyzovať, riadiť? (8)

- **Miera ovplyvniteľnosti rizika**
 - Ovplyvniteľné, Čiastočne ovplyvniteľná, Neovplyvniteľné
- **Vzt'ah k organizácii**
 - Interné riziká - tieto druhy rizík môže subjekt ovplyvňovať a riadiť, prejavujú sa vo vnútri organizácie
 - Externé riziká - tieto druhy rizík subjekt nemôže priamo ovplyvňovať, jedná sa o faktory prostredia
- **Poradie pôsobenia - vzniku a odstrániteľnosti**
 - Primárne, sekundárne - tieto druhy rizík vznikajú pri eliminácii primárnych rizík
 - Zvyškové (zostatkové, reziduálne) - tento druh rizika zostáva po eliminácii rizika, jedná sa o riziko, ktoré je subjekt ochotný niesť

Riziká – ako ich analyzovať, riadiť? (9)

- **Veľkosť rizika**
 - Malá, Stredná, Veľká
- **Miera akceptovateľnosti (prijateľnosti, únosnosti)**
 - Nevyhnutná (nutná), Únosná (prijateľná), Neúnosná (neprijateľná)
- **Pravdepodobnosť vzniku a pôsobenia**
 - Nepravdepodobná, Málo pravdepodobná, Pravdepodobná, Veľmi pravdepodobná, Takmer istá
- **Rozsah pôsobenia**
 - Systematická - tento typ rizika platí pre všetky podnikateľské subjekty
 - Nesystematické - tento typ rizika platí len pre určitý odbor podnikania

Základné princípy riadenia rizík možno teda zhrnúť do nasledujúcich tvrdení:

Každá ľudská činnosť prináša určité riziká

Nulové riziko v praxi
neexistuje!!

Aktuálne normy pre certifikáciu MS

Ktoré oblasti podnikania treba manažovať ?

- financie
- plánovanie a projektovanie
- výrobu a dodávku
- kvalitu
- bezpečnosť informácií
- požiarnu ochranu
- zákaznícky servis
- obraz a reputáciu firmy
- environment
- BOZP
- ochranu prevádzky
- ľudí
- zainteresované strany
- právne a iné predpisy

Prečo?

Ich funkčnosť, efektívnosť a účinnosť ovplyvňujú - RIZIKÁ

Ktoré oblasti podnikania treba manažovať ? (2)

Manažovanie oblastí podnikania vo výrobe a službách je v prevažnej miere kryté sofistikovanými normami pre zavádzanie/ budovanie manažérskych systémov

a následné overovanie zhody praktického dosiahnutia úrovne voči kritériálnym požiadavkám certifikačných noriem pre manažérske systémy nezávislým a objektívnym spôsobom

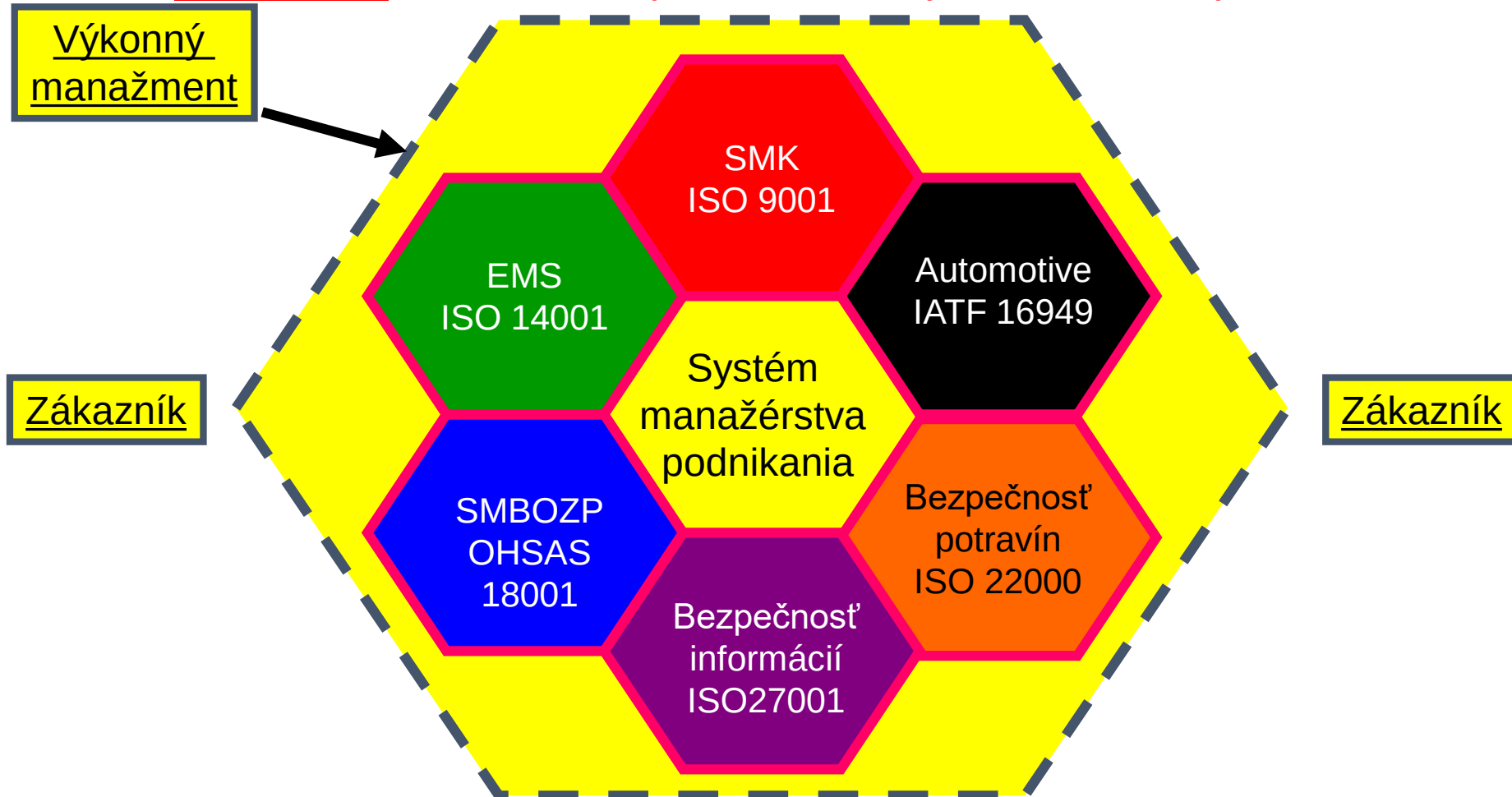
Prečo?

Integrované manažérske systémy na procesnom princípe
implementovanými nástrojmi riadenia a
monitorovania výsledkov **riadia** (eliminujú) riziká a
hrozby, aby tým **minimalizovali** zraniteľnosť firmy a
tak zabezpečili pre procesy firmy funkčnosť,
efektívnosť a účinnosť

Zabezpečili tak - svoj **ÚSPECH**

Aktuálne normy pre certifikáciu MS

Neúplný zoznam aplikovateľných noriem pre IMS



Je oprávnená váhavosť firiem k prechodu na
„nové“ certifikačné normy?

Je skutočne dôvodom obava z možného
„nezvládnutia“ požiadaviek nových verzií
noriem na riadenie rizík?

Č obsahujú požiadavky noriem z tejto oblasti?

Certifikačná norma: ISO 9001:2015

Zjednotená štruktúra požiadaviek normy a definícia striktných požiadaviek na riadenie rizík v procesoch certifikovanej spoločnosti. Nový pohľad na možnosti integrácie rôznych požiadaviek špecifických certifikačných noriem/ schém v procesoch certifikovanej spoločnosti.

- V štruktúre normy definovaný článok **6.1 – činnosti na riešenie rizík a príležitostí**
- **Aktíva** – vstup do identifikácie a priradenia relevantných rizík v procesoch spoločnosti - (vychádza z „mapy“ procesov spoločnosti)

Certifikačná norma: ISO 9001:2015

Myslenie založené na rizikách je principiálnou zmenou v ostatnej revízii normy ISO 9001.

Začlenenie požiadaviek:

- Článok 4 (Context - Kontext organizácie) – organizácia **musí identifikovať riziká**, ktoré môžu ovplyvniť **ciele**.
- Článok 5 (Leadership - Vodcovstvo) – vrcholový manažment **má záväzok** zabezpečiť realizáciu požiadavky z článku 4.
- Článok 6 (Planning - Plánovanie) – organizácia **musí identifikovať riziká a príležitosti**.

Certifikačná norma: ISO 9001:2015

Myslenie založené na rizikách je principiálnou zmenou v ostatnej revízii normy ISO 9001.

Začlenenie požiadaviek:

- Článok 8 (Operation - Prevádzka) – organizácia **musí zaviesť procesy manažérstva rizík a príležitostí.**
- Článok 9 (Performance evaluation - Hodnotenie výkonnosti) – organizácia **musí monitorovať, merať, analyzovať a vyhodnocovať riziká a príležitosti.**
- Článok 10 (Improvement - Zlepšovanie) – organizácia **musí realizovať zlepšenia** ako reakciu na zmeny **rizík.**

Certifikačná norma: ISO 14001:2015

- Zjednotená štruktúra požiadaviek normy a definícia striktných požiadaviek na riadenie rizík v procesoch dotýkajúcich sa environmentu – aspektov (aktív) a ich vplyvov. Nový pohľad na možnosti integrácie rôznych požiadaviek špecifických certifikačných noriem/ schém v procesoch certifikovanej spoločnosti.
- **V štruktúre normy definovaný článok 6.1 – činnosti na riešenie rizík a príležitostí**
- **Článok 6.1.2 Environmentálne aspekty (možno ich považovať z pojmovologického pohľadu za špecifické aktíva)**
- **Zhodne s filozofiou ISO 9001 v ostatných článkoch**

Certifikačná norma: ISO 22000 :2005

- Systémová („**stará**“!!) norma, ktorá obsahuje a dopĺňa svojou dikciou požiadavky HACCP (**H**azard **A**nalysis and **C**ritical **C**ontrol **P**oints – Systém analýzy rizika a stanovenia kritických kontrolných bodov)
- bod normy **7.4 Analýza rizík – požiadavka**
- zavedením a uplatnením garantuje vo výrobe zaistenie bezpečnosti potravín – analýza slúži pre identifikáciu a elimináciu biologických, chemických alebo fyzikálnych činiteľov / rizík, ktoré pôsobia na potravinu - a môžu porušiť jej nezávadnosť.

Certifikačná norma: ISO 22000 :2005 (2)

- Identifikovaným rizikám je lepšie predchádzať, ako ich následne odstraňovať - systém bezpečnosti potravín je založený na prevencii
- založený na nedeštrukčnej, nepretržitej kontrole materiálov, podmienok, procesov výroby a ich parametrov
- nahrádza extenzívnu laboratórnu kontrolu výrobkov
- pravidelné kontroly - sám prevádzkovateľ výroby, tie sú zamerané na dosahovanie hygienickej bezchybnosti a zdravotnej neškodnosti ním vyrábaných a ponúkaných potravín.

Certifikačné normy: ISO 22000 :2005 (3)

- na každom stupni výrobného procesu môže vzniknúť riziko ohrozujúce bezpečnosť potravín, nutné zhodnotiť závažnosť a riziko nebezpečenstva a zdravotnú závažnosť
- systém bezpečnosti potravín identifikuje konkrétne nebezpečenstvá (riziká), hodnotí ich významnosť, vyžaduje metodiku a formu riadenia rizík
- prijíma systematické opatrenia na ich kontrolu

Certifikačná norma: ISO 18001 :2007

- **Stará“** norma – pracuje systémovo s rizikami v oblasti BOZP
- V každom výrobnom, nevýrobnom procese môže vzniknúť riziko ohrozujúce bezpečnosť pracovníkov, je nutné zhodnotiť závažnosť a riziko nebezpečenstva a zdravotnú závažnosť dopadu
- systém bezpečnosti a ochrany zdravia pri práci identifikuje konkrétne nebezpečenstvá (riziká) na pracovných miestach, hodnotí ich významnosť, vyžaduje metodiku a formu riadenia rizík
- prijíma systematické opatrenia na ich kontrolu a narába s prostriedkami pre elimináciu/ zmiernenie dopadu rizík

Certifikačná norma: ISO/IEC 27001:2013

- Norma obsahuje systémové špecifikácie a požiadavky na ISMS (information security management system).
- **Narába exaktne s požiadavkami na metodické spracovanie internej dokumentácie pre identifikáciu aktív, hrozieb, riadenia rizík, hodnotenie, klasifikáciu....**
- **Vyžaduje angažovanosť vedenia pre riadenie zdrojov na elimináciu rizík, odsúhlasovanie zostatkových rizík vedením ...**
- Predpisuje aplikáciu „Opatrení v prílohe A“ Normy (Vylúčenie aplikácie opatrení - povinne zdôvodniť)

Certifikačná norma: ISO/TS 16949:2009 IATF 16949:2016

- Norma obsahuje základ – 9001 + systémové špecifikácie a požiadavky na dodávateľov pre oblasť Automotive
- Predpisuje spracovanie metodiky pre výkon analýzy rizík v procesoch spoločnosti, identifikáciu a riadenie pre riziká v uplatnení špecifických požiadaviek zákazníkov, riziká v oblasti zodpovednosti za vady výrobku uvádzaného na trh, riziká v spojení s používaním materiálov zodpovedajúcich legislatívnym požiadavkám.
- Definuje povinné používanie metodológie FMEA pre riadenie rizík projektov vývoja a metódu 5x WHY? pre identifikáciu príčin vzniku nezhody.

A takto sa javí aktuálny stav z
pohľadu audítorov

=

PRAX

Certifikačná norma: ISO 9001:2015 (1)

- Prevažná väčšina (cca 90%) certifikovaných subjektov zostáva v procese certifikácie podľa „starej“ verzie normy
- Nie je metodicky a ani vecne doriešené spracovanie tém týkajúcich sa riadenia rizík v procesoch spoločností
- **Uvažovanie zohľadňujúce riziká** umožňuje síce organizácii **určiť faktory**, ktoré by mohli spôsobiť v procesoch a jej systéme manažérstva kvality odchyľovanie od plánovaných výsledkov, aby sa zaviedli **preventívne opatrenia** s cieľom minimalizovať negatívne dopady a aby sa max. využili príležitostí, ktoré sa vyskytnú

Certifikačná norma: ISO 9001:2015 (2)

- Prvocertifikované firmy majú síce aktívne spracovanú „nekonečnú“ databázu rizík, no ich hodnotenie, prioritizácia a riadenie je problémom. NEVEDIA, čo s rizikami ďalej robiť !!!!!
- Monitorovanie a meranie ukazovateľov výkonnosti, ktoré sú nutné pre riadenie a sú špecifické pre každý proces a líšia sa v závislosti na **procesných rizikách nie sú v praxi zavedené**.
- Formy pre identifikáciu aktív a k nim priradených rizík nie sú dostatočne zvládnuté ani poradenskými spoločnosťami
- Platí to aj pre zavedené IMS

Certifikačná norma: ISO 14001:2015

- S aktívami (aspektami) v oblasti environmentálneho manažérstva spoločnosti pracovali aj počas platnosti predchádzajúcej normy – no zmena filozofie a prístupu.
- Kriteriaálne posudzovanie identifikovaných rizík k jednotlivým aktívam (aspektom), vzhľadom na požiadavky normy - rozpracovať opatrenia do stratégie, dlhodobých a krátkodobých cieľov **nie je však na požadovanej úrovni**
- Niektoré druhy hrozieb nie sú dostatočne v systémoch identifikované, hlavne tie, vyplývajúce z neplnenia legislatívnych požiadaviek a rozhodnutí orgánov štátnej správy (určené záväzné limity)....

Certifikačná norma: ISO 22000 :2005

- Keďže povinnosť mať zavedený funkčný systém HACCP (Hazard Analysis and Critical Control Points – Systém analýzy rizika a stanovenia kritických kontrolných bodov) je požiadavkou danou na slovensku povinne zo zákona o potravinách č.152/1995 Z. z. a VIII. hlavou Potravinového kódexu
- bod normy 7.4 Analýza rizík – požiadavka je v každom prípade naplnená aj vecne, riziko sankcií od dozorných orgánov štátu je dostatočným argumentom k udržiavaniu funkčného systému a aktualizáčnym zmenám
- problémom je hľadanie koreňových príčin incidentov a riešenie prijímaním opatrení, ktoré neodstraňujú dôsledok

Certifikačná norma: ISO 18001 :2007

- Zákon 124/2006 v znení neskorších predpisov určuje požiadavky na BOZP pre pracovníkov.
- Na základe požiadavky zákona spoločnosti za podpory systémových požiadaviek pracujú systémovo s rizikami v oblasti BOZP – problém externé dodávky
- Ďalšie povinnosti dané zákonom (evidencia, analýza neželaných udalostí, pracovných úrazov) v kombinácii s procesným modelom umožňujú v princípe plniť požiadavky aj pre certifikačnú normu.
- Sú podceňované riziká v spojení s chýbajúcimi teoretickými a praktickými skúsenosťami pracovníkov v oblasti prevencie - povedomie k bezpečnosti.

Certifikačná norma: ISO/IEC 27001:2013

Plnenie požiadaviek na riadenie rizík je pre túto certifikačnú normu naplnené zrejme najlepšie

- Spoločnosti majú v prevažnej miere podrobne spracované metodiky k jednotlivým požadovaným oblastiam
- Identifikácia aktív a aktualizácia zoznamov s následným hodnotením rizík k aktívam, nasadzovanie opatrení, monitorovanie incidentov a hľadanie príčin ich vzniku je prakticky zavedené štandardné prostredie prevádzkovania ISMS v procesoch spoločností
- V poslednom období je problémom kategorizácia dokumentov vedených v papierovej forme (aktíva)

Certifikačná norma: ISO/TS 16949:2009 IATF 16949:2016

- Striktné a jednoznačné požiadavky na dokumentáciu, metodiky a výkon činností spoločne s aktívnym dohľadom zákazníkov zabezpečujú vysokú efektívnosť v tejto oblasti certifikácie
- Výsledky dopadov rizík, analýzy vzniku problémov je spoločne s rozširujúcou sa komunikáciou on-line systémov prostredie pre akceptáciu, alebo zamietnutie opatrení.
- Núti certifikované spoločnosti vzhľadom na vysoké podnikateľské riziko viesť vyspelý a sofistikovaný spôsob riadenia rizík v jednotlivých interných a aj externe zabezpečovaných procesoch

Spoločné požiadavky certifikačných noriem na manažérske systémy

- Neustále zlepšovanie (PDCA cyklus)
- Úloha vedenia, ciele, hodnotenie funkčnosti
- Identifikácia procesov
- Požiadavka na zdroje
- Dokumentované informácie a záznamy
- Interakcia s okolím (rozhrania do externých procesov)
- Identifikácia rizík a riadenie dopadov rizík na procesy spoločnosti a cez rozhrania – hrozby
- Náprava a zlepšovanie

**Riziká priniesla dynamizujúca sa doba a
meniace sa požiadavky zákazníkov**

**Nie je možné dlhodobo ignorovať dopady
rizík a identifikáciu hrozieb**

**Prežijú len tí – ktorí dokážu riadiť riziká pre
podnikanie v reálnom čase**

**Požiadavky noriem a metódy riadenia
sú vhodným prostriedkom**

Ďakujem za pozornosť

Ing. Pavel Horník

pavel.hornik@tuv-sud.sk



eFOCUS