# Systém řízení informační bezpečnosti

Information security management systém

*Luděk Novák, Josef Požár*[1]

## 1. Úvod

Na informační bezpečnost se dá nahlížet z různých úhlů a obecně tento pojem zahrnuje celou řadu problémů a jejich řešení. Zabezpečení sítě, fyzických spojů a serveru, kódování datových přenosů, digitální podpis, dodržování firemních směrnic, autentizace, autorizace, autenticita, nepopiratelnost, antivirová a antispamová ochrana, hodnocení a ochrana firemních aktiv, analýza rizik, zálohování, obnova po chybě a další. Cílem tohoto pojednání jeseznámit čtenáře s metodikou ustanovení, zavádění a zajištění provozu, monitoringu a údržby systému řízení informační bezpečnosti (dále jen ISMS - Information Security Management System) v organizaci. ISMS lze zavést a používat v organizaci s deseti pracovníky, a stejně tak i ve velkém holdingu, který může čítat tisíce zaměstnanců. Zjednodušeně lze říci, že ISMS je jen jeden a to ten, který je popsán v normě ISO/IEC 27001. Interpretace a implementace jednotlivých doporučení se však může výrazně lišit podle rozsahu systému, počtu uživatelů, způsobu zpracování dat, jejich hodnoty a především podle reálných bezpečnostních rizik apod. Strategie ISMS nebývá v malých a středních firmách popsána tak detailně, jako je tomu zvykem ve velkých, zejména nadnárodních organizacích.

ISMS se netýká jen průmyslových podniků a privátních organizací, ISMS se týká všech organizací včetně veřejně právních institucí a orgánů státu. Toho důkazem je i existence mnoha národních vládních a resortních usnesení doporučujících anebo vyžadujících implementaci ISMS v organizacích řízených a zřízených státem.

## 2. Pojem systému řízení informační bezpečnosti

Tento článek se zabývá vybranými aspekty managementu a informační bezpečnosti. Informační bezpečnost je dnes již nezbytnou součástí každého informačního systému v každé organizaci. Jedná se o důležitou součást fungování podniku i státní organizace a stává se tak integrální součástí strategie každé organizace.

V dnešní době se žádná organizace nemůže obejít bez řízení bezpečnosti informací. Bezpečnost se stala nedílnou součástí každodenního řízení a vnitřní kultury organizace. Abychom byli schopni řízení bezpečnosti cíleně a účinně a účelně rozvíjet, je potřebné na tento prvek řízení pohlížet jako na systém řízení bezpečnosti informací.

**ISMS (Information Security Management System)** – část celkového systému řízení organizace, založená na přístupu (organizace) k rizikům činností, která je zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací[2] [ISO_27001].

ISMS je soubor pravidel a opatření, po jejichž zavedení má správné a úplné informace (princip integrity) včas k dispozici ten, kdo je skutečně potřebuje (princip dostupnosti) a pouze ten, kdo je k přístupu k nim oprávněn (princip důvěrnosti).

---

[1] Ing. Luděk Novák, Ph.D. – senior konsultant ANECT, a.s., doc. RNDr. Josef Požár, CSc. – děkan fakulty bezpečnostního managementu, Policejní akademie České republiky v Praze.

[2] Systém řízení v sobě zahrnuje organizační strukturu, politiky, plánovací činnosti, odpovědnosti, mechanismy, postupy, procesy a zdroje.

ISMS je efektivní dokumentovaný systém řízení a správy informačních aktiv s cílem eliminovat jejich možnou ztrátu nebo poškození tím, že jsou určena aktiva, která se mají chránit, jsou zvolena a řízena možná rizika bezpečnosti informací, jsou zavedena opatření s požadovanou úrovní záruk a ta jsou kontrolována. ISMS může být zaveden pro organizační složku instituce, informační systém nebo jeho část, případně může zahrnovat celou organizaci.

Řízení bezpečnosti informací a systém řízení bezpečnosti informací jsou v neustálé pozornosti všech manažerů, kteří během své práce přicházejí do syku s daty, zpracovávanými pomocí informačních a komunikačních technologií.

ISMS je systém, který nejen chrání informace organizace před ztrátou či zneužitím, ale chrání i členy vedení a zaměstnance před nechtěnými prohřešky vůči zákonům ČR.

Bezpečnost informací je spojená s distribuovanou (individuální) zodpovědností a je velmi důležitá pro zajištění činností jakékoli organizace. Největším nebezpečím pro zabezpečení informací je člověk, který způsobí většinu bezpečnostních incidentů.

Každý si musí být vědom toho, že se nedá bezpečnost informací zajistit stoprocentně, ale mělo by být provedeno vše, aby se bezpečnost zajistila na přijatelné úrovni za ekonomicky zdůvodnitelné náklady. A právě zde sehrává nezastupitelnou roli řízení rizik, které je nenahraditlným základem každého ISMS.

## 3. Důvody a rámec[3] řízení informační bezpečnosti

Budování informační bezpečnosti představuje trvalou soustavu činností. Vlastní zajištění informační bezpečnosti je proces, který je nutné řídit tak jako kterýkoliv jiný proces.

ISMS tvoří součást řídících činností organizace. Jak již bylo uvedeno cílem ISMS je plně vyloučit nebo alespoň snížit rizika související s možným narušením integrity, dostupnosti a důvěrnosti informací organizace.

Úkolem ISMS je zavést pravidla a postupy pro řízení informační bezpečnosti organizace. Pro ISMS v rámci organizace musí být jednoznačně popsána organizace řízení, odpovědnost za informační bezpečnost řídících pracovníků všech stupňů, odborných orgánů a rolí v systému bezpečnosti informací.

Z důvodu zajištění dostatečné efektivity bezpečnosti informací se musí jednat o řízený proces vyvážený ve všech oblastech, který má podporu vedení a respektuje kulturu organizace. Z ekonomického hlediska se musí jednat o zajištění informační bezpečnosti za „ospravedlnitelné“ náklady.

V organizační struktuře organizace musí být informační bezpečnost zohledněna tak, aby pokrývala činnosti a spolupráci vedení, osob odpovědných za aplikační systémy, provozní služby, koncové uživatele a osoby odpovědné za jednotlivé činnosti. Informační bezpečnost předpokládá úzkou spolupráci všech uvedených skupin pracovníků a poskytování školení v oblasti informační bezpečnosti, tak aby kromě osob, které v organizaci odpovídají za informační a další bezpečnost, měli základní znalosti o informační bezpečnosti i pracovníci pracující ve správě informací a všichni uživatelé informační techniky.

Hlavním cílem systému řízení informační bezpečnosti je provádět vhodná opatření, jejichž účelem je vyloučení nebo minimalizace dopadu různých bezpečnostních hrozeb. S těmito hrozbami souvisejí také zranitelnosti, které mohou působení hrozeb negativně ovlivnit. Přitom

[3] Framework. The ISMS Framework Dostupné na WWW:
< http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/rm-isms/framework>

řízení informační bezpečnosti umožní realizaci žádoucí kvalitativní vlastnosti služeb nabízených organizací tj. dostupnost služeb, zachování důvěrnosti a integrity dat atd.

Rámec ISMS je dán nejen velikostí, ale zejména počtem a kvalitou konkrétních procesů a aktivit organizace a reálnými riziky. To umožňuje stanovit další aspekty bezpečnostních požadavků jako právní, regulační na dané provozní úrovni.

Malé organizace s omezenou infrastrukturou informačních systémů, jejichž provoz nevyžaduje manipulace, skladování a zpracování osobních či důvěrných údajů, mívají většinou menší rizika tj. rizika s nižší pravděpodobností výskytu a s nižšími negativními dopady. Malé organizace udržují nezávislý ISMS, který řeší bezpečnostní rizika ad hoc, nebo jsou součástí širšího procesu řízení rizik.

Velké organizace jako jsou banky a finanční instituce, telekomunikační operátoři, nemocnice a zdravotnické instituce a veřejné či státní orgány, mají velmi mnoho důvodů ke komplexnímu řešení informační bezpečnosti. Právní a regulační požadavky, jejichž cílem je ochrana citlivých nebo osobních údajů, musí věnovat velkou pozornost rizikům bezpečnosti informací.

Za těchto okolností je vývoj a implementace samostatného a nezávislého procesu ISMS velmi důležitou a jedinou alternativou. Vývoj rámce ISMS zahrnuje následující body:

- vymezení působnosti ISMS,
- definice bezpečnostní politiky,
- hodnocení rizika (jako součást Risk Management),
- management řízení rizik,
- výběr vhodných opatření a
- prohlášení o aplikovatelnosti.

Během celého procesu jsou hodnocena rizika a řízení procesu, které tvoří jádro ISMS. Tyto procesy, které lze "transformovat" na jedné straně pravidla a obecné bezpečnostní politiky a cíle a na druhé straně transformovat cíle do ISMS konkrétní plány pro provádění kontrol a mechanismy, jež jsou zaměřeny na minimalizaci hrozeb a zranitelnosti. Za zmínku stojí, že tyto body jsou mnohdy považovány za jeden subjekt, který se mnohdy označuje také jako Risk Management.

Procesy a činnosti související se netýkajípouze informačních rizik. Jsou to spíše operativní opatření k zajištění technické realizace, údržby a kontroly bezpečnostních měření.

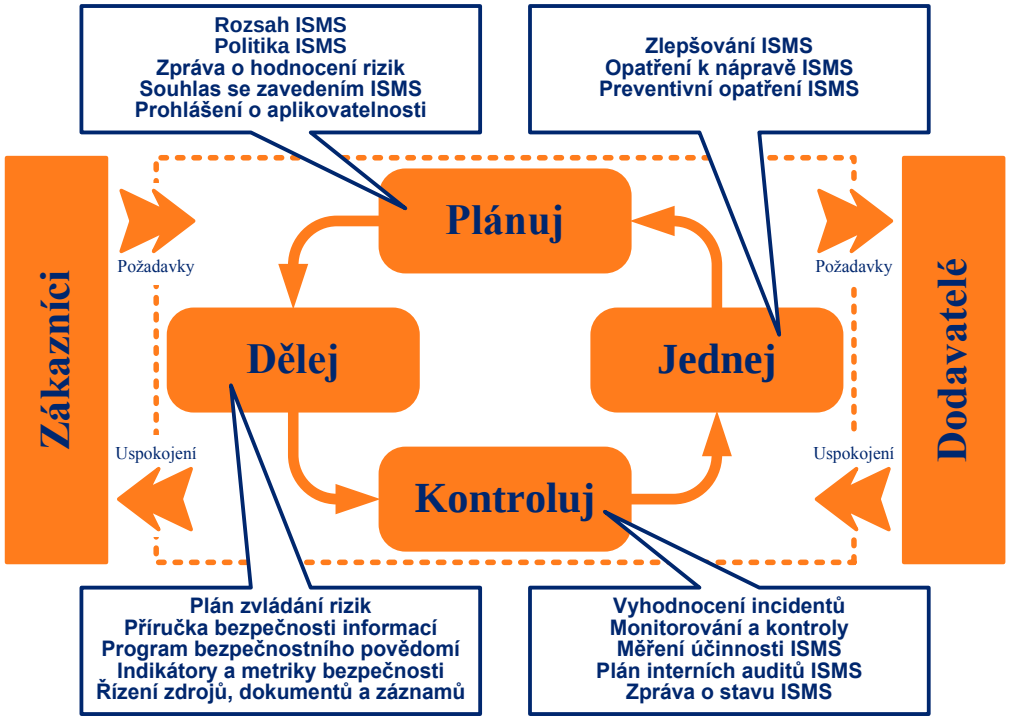
Vhodné kontroly mohou být buď z existujících (vyčerpávající) sady ovládacích prvků nebo mechanismů, obvykle zahrnuta v normách bezpečnosti informací (např. ISO/IEC 27001-Specifikace systémů řízení informační bezpečnosti) a dalšími pokyny. Tyto kontroly mohou být rovněž výsledkem kombinace a úpravy navrhovaných kontrol specifické organizační požadavky nebo provozní vlastnosti.

ISMS se tak stává cyklickým stále opakujícím procesem Zavedení bezpečnostní politiky a vymezení působnosti ISMS je častěji se opakující proces řízení strategických cílů. Naopak proces řízení rizik je každodenní provozní činnost.

## 4. Model ISMS

Systém řízení bezpečnosti informací je podobně jako ostatní systémy řízení založen na modelu PDCA (Plánuj – Dělej – Kontroluj – Jednej). Využití tohoto modelu pro ISMS je zachyceno na obrázku Na obrázku 1 jsou definovány následující čtyři etapy celého životního cyklu systému řízení:

- **Ustanovení ISMS** – cílem této etapy je upřesnit rozsah a hranice, kterých se řízení bezpečnosti týká, stanovit jasné manažerské zadání a na základě ohodnocení rizik vybrat nezbytná bezpečnostní opatření.
- **Zavádění a provoz ISMS** – cílem této etapy je účelně a systematicky prosadit vybraná bezpečnostní opatření do chodu organizace.
- **Monitorování a přezkoumání ISMS** – hlavním cílem této etapy je zajištění zpětné vazby a pravidelného sledování a hodnocení úspěšných i nedostatečných stránek řízení bezpečnosti informací.
- **Údržba a zlepšování ISMS** – cílem poslední etapy je realizace možností zlepšování systému řízení bezpečnosti informací ať už soustavným zlepšování systému nebo odstraňování zjištěných slabin a nedostatků.




**Obr. 1: PDCA Model pro řízení bezpečnosti informací [ISO27001]**

## 4.1 Ustanovení ISMS

První etapou budování ISMS je jeho ustanovení, při kterém jsou upřesněny správné formy řešení bezpečnosti informací. Kromě definice rozsahu ISMS a odsouhlasení **Prohlášení o politice ISMS** (závazek vedení podniku podporovat informační bezpečnost) patří mezi kritické činnosti provedení analýzy rizik a výběr vhodných bezpečnostních opatření pro snížení vlivu existujících rizik. Tato etapa prosazování ISMS by měla být ukončena souhlasem vedení se zavedením ISMS podle potřeb organizace zjištěných při analýze a zvládání rizik ISMS.

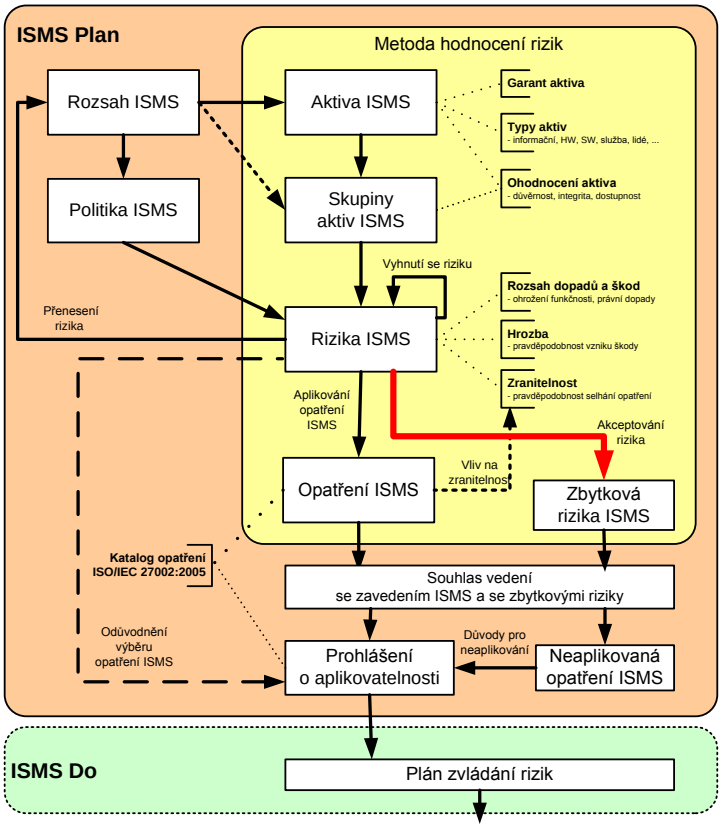
Ustanovení ISMS je možné rozdělit na následující skupiny činností:

- definice rozsahu, hranic a vazeb ISMS,
- definice a odsouhlasení Prohlášení o politice ISMS,
- analýza a zvládání rizik,
  - definice přístupu organizace k hodnocení rizik,

- identifikace rizika včetně určení aktiv a jejich vlastníků,
- analýza a vyhodnocení rizik,
- identifikace a ohodnocení variant pro zvládání rizik,
- výběr cílů opatření a jednotlivých opatření pro zvládání rizik,
- souhlas vedení organizace s navrhovanými zbytkovými riziky a se zavedením ISMS,

- příprava Prohlášení o aplikovatelnosti.

Etapa ustanovení ISMS je důležitou etapou budování ISMS, protože definuje základy celého systému řízení bezpečnosti informací. Zrádnost této etapy je dána především tím, že výsledky etapy se intenzivně promítají do dalších etap, kde mají dlouhodobější vliv, a navíc mnoho řešitelů není dostatečně připraveno na budování ISMS a některé souvislosti jim docházejí až v dalších etapách, kdy už je provedení změn náročnější a určitě vyžaduje větší úsilí a větší finanční náklady.




**Obr. 2: Řízení rizik v procesu ISMS (Doucek 2011)**

Systémový význam etapy ustanovení ISMS je zřejmý z Obr. 2, na kterém je podrobně zachycen postup činností a základní souvislosti. Budování ISMS začíná vlevo nahoře určením rozsahu ISMS, který přímo ovlivňuje politiku ISMS a aktiva, která jsou do ISMS zahrnuta a z nichž se, pro větší přehlednost, vytvářejí skupiny aktiv s obdobnými bezpečnostními parametry. Toto vše určuje potřeby ISMS, jimž se musí návrh ISMS podřídit.

Míra, do jaké jsme schopni potřebám ISMS vyhovět, je dána riziky ISMS. S těmi je možné pracovat následujícími způsoby. Buď se riziku vyhneme a měníme tak potřeby ISMS tím, že se snížily dopady dané hrozby či pravděpodobnost jejích výskytu. Při přenesení rizika, další varianta jeho zvládání, se mění rozsah ISMS, protože musí být doplněn subjekt, na který bylo riziko přeneseno (např. pojišťovna). Nejčastější formou zvládání rizika je aplikace vhodného bezpečnostního opatření, což má vliv na snižování zranitelnosti u daného rizika. Poslední

možností zvládání je akceptace rizika, což je vlastně vždy konečný výsledek zvládání rizik. Tato forma zvládání rizik v sobě skrývá zbytková rizika, která by měla být zaznamenána.

Poslední kroky plánování vedou k zajištění formálního souhlasu vedení organizace s výběrem opatření a se zbytkovými riziky. Bezpečnostní manažer na tomto základě může zpracovat prohlášení o aplikovatelnosti a připravit plán na zvládání rizik. To se ale už dostáváme do další části PDCA cyklu, kterou je zavedení ISMS.

**Etapa ustanovení ISMS má zásadní dopady na fungování ISMS během jeho celého životního cyklu.**

## 4.2 Zavádění a provoz ISMS

Tato etapa životního cyklu ISMS se soustředí na prosazení všech bezpečnostních opatření tak, jak byla navržena v předchozí etapě při ustanovení ISMS. Důležité je především připravit dílčí plány, kde jsou upřesněny termíny, odpovědné osoby apod. Všechna bezpečnostní opatření by měla být zdokumentována v tzv. **Příručce bezpečnosti informací** a mělo by dojít k vysvětlení bezpečnostních principů všem uživatelům a manažerům.

Během této etapy zavádění ISMS je nezbytné provést následující činnosti:

- Formulovat dokument plán zvládání rizik a započít s jeho zaváděním.
- Zavést plánovaná bezpečnostní opatření a zformulovat příručku bezpečnosti informací, která upřesní pravidla a postupy aplikovaných opatření v definovaných oblastech bezpečnosti informací (viz ISO/IEC 27002).
- Definovat program budování bezpečnostního povědomí a provést přípravu a zaškolení všech uživatelů, manažerů a odborných pracovníků z úseku informatiky a zejména z oblasti řízení bezpečnosti.
- Upřesnit způsoby měření účinnosti bezpečnostních opatření a sledovat stanovené ukazatele.
- Zavést postupy a další opatření pro rychlou detekci a reakci na bezpečnostní incidenty.
- Řídit zdroje, dokumenty a záznamy ISMS.

## 4.3 Monitorování a přezkoumání ISMS

Hlavním úkolem této etapy zavádění ISMS je zajistit účinné zpětné vazby. V souvislosti s tímto požadavkem by proto mělo dojít k prověření všech aplikovaných bezpečnostních opatření a jejich důsledků na ISMS. Vlastní ověření začíná u přímé kontroly odpovědných osob ze strany jejich nadřízených či bezpečnostním manažerem. Důležitou roli sehrává též nezávislé posouzení fungování a účinnosti ISMS pomocí interních auditů ISMS. Obecným cílem všech použitých zpětných vazeb je připravit dostatek podkladů o skutečném fungování ISMS, které budou předloženy vedení za účelem přezkoumání, zda je realizace ISMS v souladu s obecnými potřebami organizace. Během této části zavádění ISMS je nezbytné provést následující činnosti:

- monitorovat a ověřit účinnost prosazení bezpečnostních opatření,
- provést interní audity ISMS, jejichž náplň pokryje celý rozsah ISMS,
- připravit zprávu o stavu ISMS a na jejím základě přehodnotit ISMS na úrovni vedení organizace (včetně revize zbytkových a akceptovaných rizik).

## 4.4 Údržba a zlepšování ISMS

Poslední etapou celého cyklu prosazování ISMS je jeho udržování a zlepšování. Jedná se především o to, že v této fázi by mělo docházet ke sběru podnětů ke zlepšení ISMS a k nápravě všech nedostatků tzv. neshod, které se v ISMS objevují.

Během této části zavádění je nezbytné provést následující činnosti:

- zavádět identifikované možnosti zlepšení ISMS (především na základě přehodnocení vedením),
- provádět odpovídající opatření k nápravě a preventivní opatření pro odstranění nedostatků.

**Neshoda (Nonconformity)** – nesplnění požadavku [ISO_9000].

**Náprava (Correction)** – opatření pro odstranění zjištěné neshody [ISO_9000].

**Opatření k nápravě (Corrective action) –** opatření k odstranění příčiny zjištěné neshody nebo jiné nežádoucí situace [ISO_9000].

**Preventivní opatření (Preventive action)** – opatření k odstranění příčiny potenciální neshody nebo jiné nežádoucí potenciální situace [ISO_9000].

## 4.5 Praktická doporučení

Při budování systému řízení bezpečnosti informací je nezbytné realizovat celý životní cyklus ISMS, definovaný v ISO/IEC 27001:2005. Tento postup je nezbytný pro případy certifikace ISMS podle této normy, nicméně i v případě nižších ambicí lze dodržování pravidel norem jen doporučit. Životní cyklus ISMS představuje vybudování ISMS, jeho zavedení a provoz, monitorování a přehodnocování ISMS a jeho udržování a zlepšování. Všechny činnosti by měly být nejen řádně provedeny, ale i náležitě formalizovány pomocí dokumentů či záznamů ISMS. Pro úspěšné zavedení ISMS jsou klíčové především následující součásti ISMS:

- **Působnost ISMS** – vymezení rozsahu a hranic ISMS na základě požadavku organizace a určení, které části organizace mají má být do ISMS zahrnuty. Působnost ISMS vychází z cílů a strategie organizace.
- **Prohlášení o politice ISMS** – stanovuje celkový směr realizace ISMS a určuje cíle a strategii ISMS. Dále vymezuje požadavky, které působí na ISMS (legislativní požadavky, vazby na podnikatelské činnosti organizace a smluvní závazky organizace apod.) a ustavuje kritéria pro hodnocení rizik. Politika by měla tvořit jasný a jednoduchý dokument na vyšší úrovni abstrakce.
- **Analýza a zvládání rizik** – představuje základní kámen systému řízení, od kterého jsou odvozována všechna bezpečnostní opatření, jejich účinnost a účelnost. I přesto, že bezpečnostní analýza je velmi důležitá, nejsou vyžadovány žádné speciální techniky. Ze zkušeností je potřeba jen doplnit, že méně je někdy více.
- **Prohlášení o aplikovatelnosti** – je důležitým dokumentem, který upřesňuje bezpečnostní opatření, která jsou či budou aplikována systémem řízení bezpečnosti informací. Při tvorbě tohoto dokumentu je důležité pečlivě zvažovat vybíraná opatření s ohledem na náročnost (finanční, personální apod.) jejich realizace.
- **Plán zvládání rizik** – vymezuje řídicí činnosti, odpovědnosti a priority pro řízení rizik bezpečnosti informací. Na základě tohoto dokumentu probíhá další zavádění ISMS v organizaci.
- **Záznamy**[4] – jsou hlavním prvkem systému řízení, kterým se prokazuje jeho správné fungování. Tuto skutečnost je nutné mít při budování systému řízení na paměti, a proto je důležité všechny definované procesy navrhnout tak, aby vždy poskytovaly příslušné záznamy o jejich průběhu a tyto záznamy skutečně vytvářet.

[4] Záznamem se rozumí doklad o tom, že byla provedena určitá činnost včetně informací o obsahu a výsledku dané činnosti.

- **Přehodnocení** – je pravidelný úkon, při kterém jsou výsledky ISMS prezentovány vedení organizace. Jeho hlavním cílem je seznámit vedení se stavem řízení bezpečnosti v organizaci a upřesnit plán a následný postup na další období (většinou na jeden rok).

Výše uvedené prvky jsou důležitými částmi řešení ISMS, které by neměly být opomenuty a měly by být dobře zvládnuty. Nicméně samotné budování ISMS nelze zúžit pouze na ně, neboť zavedení ISMS se odvíjí od potřeb a charakteru ochraňovaných informací.

## 5. Realizace bezpečnostních opatření

Druhým základním východiskem ISMS je norma ISO/IEC 27002:2005 - Soubor postupů pro řízení bezpečnosti informací (dříve ISO/IEC 17799). Ta obsahuje tzv. nejlepší zkušenosti řízení bezpečnosti informací. Její revidované vydání bylo publikováno v červnu 2005. Doporučení normy obsahuje 133 bezpečnostních opatření, která jsou rozdělena do 11 oblastí – viz Obr. 3.


**Obr. 3: Oblasti bezpečnosti informací [ISO27002]**

Jednotlivé oblasti se věnují následujícím skupinám bezpečnostních opatření:

- **Bezpečnostní politika –** definice základních pravidel bezpečnosti informací a vyjádření podpory vedením organizace.
- **Organizace bezpečnosti** – upřesnění struktury pro řízení bezpečnosti informací uvnitř organizace a řízení bezpečnosti ve vztahu k externím subjektům (zákazníkům, dodavatelům atd.).
- **Řízení aktiv** – udržování přehledu o existujících aktivech organizace a stanovení odpovědnosti za udržování přiměřené míry ochrany jednotlivých aktiv.
- **Bezpečnost z hlediska lidských zdrojů** – vymezení povinností za ochranu informací u všech pracovníků a zajištění potřebného bezpečnostního povědomí.
- **Fyzická bezpečnost a bezpečnost prostředí** – definice pravidel pro přístup osob do klíčových prostor organizace a ochrana zařízení zejména zařízení ICT (prostředí).
- **Řízení komunikací a řízení provozu** – zajištění spolehlivého a bezpečného chodu produkčních informačních a komunikačních systémů organizace.
- **Řízení přístupu** – pravidla pro přidělování přístupu ke všem prostředkům informačních a komunikačních systémů, včetně sledování způsobu využívání dostupných prostředků.

- **Akvizice, vývoj a údržba informačních systémů** – prosazení principů bezpečnosti informací do projektů rozvoje ICT a dalších podpůrných aktivit.
- **Zvládání bezpečnostních incidentů** – pravidla a postupy určené pro řešení bezpečnostních incidentů včetně shromažďování potřebných důkazů.
- **Řízení kontinuity činností organizace** – postupy prevence a minimalizace škod plynoucích pro organizaci z havárií, živelných pohrom či jiných mimořádných událostí.
- **Soulad s požadavky** – organizace dokladuje naplnění požadavků vyplývajících z právních, smluvních a jiných závazků.

Užitečný je přístup k formálnímu uspořádání normy. Ve starších verzích byla všechna bezpečnostní doporučení uvedena jako nestrukturovaný text, což nebylo pro uživatele příliš přehledné. Současná podoba rozlišuje následující tři typy popisu opatření:

- **Definice opatření** jsou jednověté specifikace bezpečnostních opatření, které jsou shodné s přílohou A normy ISO/IEC 27001:2005.
- **Směrnice pro zavedení** obsahuje podrobný popis toho, co je opatřením myšleno a jakým způsobem by opatření mělo být implementováno a prosazováno. Uvedené informace nemusí být platné pro všechny případy nasazení a je přípustné aplikovat i jiné metody řešení.
- **Další informace** soustředí specifické údaje, které by měly být při implementaci zvažovány (např. právní důsledky, odkazy na specifické bezpečnostní normy apod.).

Hlavním důvodem použití této vnitřní struktury je snaha o jednoznačné odlišení definice opatření od doporučení, jakou formou dané opatření zavádět a prosazovat. To velmi usnadňuje použití normy hlavně pro uživatele, jejichž hlavní profesní orientací není bezpečnost informací.

## 6. Závěr

Zavedení ISMS představuje větší či menší zásah do činnosti organizace a bez opravdového zájmu vedení je obtížné ISMS zdárně zavést a provozovat. Systém řízení bezpečnosti informací je základem pro účelné a účinné řízení bezpečnosti informací. Systém řízení se opírá o čtyři hlavní systémové etapy. Při **první etapě,** zavádění ISMS, je snahou vše správně „naplánovat“. Počátkem je určením rozsahu řízení a stanovení základního rámce řízení bezpečnosti informací pomocí politiky ISMS. Plánování pokračuje identifikací a ohodnocením rizikových scénářů, které vede k výběru vhodných bezpečnostních opatření. Koncem počáteční etapy řízení bezpečnosti je formulace prohlášení o aplikovatelnosti a získání souhlasu vedení organizace se zavedením ISMS.

**Druhá etapa** se soustředí na prosazení ISMS. Zde je důležité stanovit dílčí, roční plány na zvládání rizik, definovat dlouhodobě platná bezpečnostní pravidla, tato pravidla vysvětlovat všem účastníkům a sledovat účinnost, s jakou je bezpečnost prosazována.

**Třetí etapou** je zpětná vazba, která má základ v pravidelné kontrole pověřených osob. Dalším důležitým prvkem jsou interní audity ISMS. Všechny získané poznatky o ISMS jsou pak vedením organizace vyhodnoceny a vedou ke zpřesnění cílů ISMS pro další období.

Poslední **čtvrtá etapa** se věnuje soustavnému zlepšování ISMS. Krom odstraňování jeho nedostatků je hlavní výzvou využití všech nápadů, které dovolí zjednodušit a zkvalitnit systém řízení.

**Vždyť je to vlastně úplně jednoduché. Stačí jen začít!**

## Literatura

ČSN ISO/IEC 27001:2006 Informační technologie - Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky, ČESKÁ TECHNICKÁ NORMA ICS 35.040

DOUCEK, Petr; NEDOMOVÁ, Lea; NOVÁK, Luděk; SVATÁ, Vlasta. *Řízení bezpečnosti informací.* Druhé přepracované vydání, Praha : Professional Publishing, 2011, ISBN 978-80-7431-050-8, v tisku.

POŽÁR, Josef. Systém řízení informační bezpečnosti. *In Kný, Milan; Požár, Josef. Aktuální pojetí a tendence bezpečnostního managementu a informační bezpečnosti.* Brno : Tribun EU, 2010, s. 93 – 110. ISBN 978-807399-067-1.