RAM
(Risk Analysis Manager)

pragodata

Nástroj pro správu systému řízení bezpečnosti informací (ISMS) a rizik (IRMS)
S jeho pomocí si pro svůj bezpečnostní tým vytvoříte platformu, která Vám umožní jednoduchou správu a řízení aktiv, rizik a související bezpečnostní dokumentace. Pomocí systému RAM můžete efektivně analyzovat zranitelnosti, rizika, plánovat opatření a vyhodnocovat jak jejich účinnost, tak i stav systému řízení bezpečnosti jako celku.

Náš tým specialistů se bezpečnosti informačních systémů věnuje více než 20 let. Nedílnou součástí této oblasti je bezpečnost dat - primárních aktiv. Jedná se o klíčovou problematiku ve všech IT produktech.

Zaměřujeme se zejména na oblasti bezpečnosti definované normami ISO 27k, ISO 22301, ISO 31000, zákonem č. 181/2014 Sb. o kybernetické bezpečnosti a zákonem č. 253/2008 Sb. o legalizaci výnosů z trestné činnosti (AML), v rámci kterých působí i naši certifikovaní specialisté.

Řízení rizik informací
Pomůžeme Vám zavést procesy řízení rizik do Vaší organizace tak, aby nevytvářely negativní dopady, jako jsou složitá administrativa, vysoká cena bezpečnostních opatření a aby Vám pomáhaly identifikovat existující zranitelnosti a efektivně na ně reagovat vhodnými a účinnými opatřeními. Poskytneme Vám nástroje pro řízení rizik ověřené reálným provozem.

Řízení bezpečnosti informací
Pomůžeme Vám s vytvořením systému bezpečnosti informací ve Vaší organizaci, a to jak v oblasti řízení bezpečnosti informačních systémů a implementaci technologií, tak i při tvorbě bezpečnostní dokumentace a přípravě havarijních plánů. Poskytneme Vám nástroje pro správu dokumentace, řízení aktiv a zavádění bezpečnostních opatření.

Řízení kontinuity činností
Řízení kontinuity činností se zaměřuje na kritické podnikové procesy, definuje aktivity pro snížení rizika vzniku rušivé události. Cílem je zabezpečit kritické procesy v organizaci při vzniku rušivé události. Pomůžeme Vám vytvořit strategii kontinuity činností a plány na zachování kontinuity činností Vašich klíčových procesů. Poskytneme Vám nástroje pro zvládání rušivých událostí a sdílení krizových postupů.

Řízení kybernetické bezpečnosti
Pomůžeme Vám s vytvořením systému řízení kybernetické bezpečnosti ve Vaší organizaci dle platného právního rámce, a to jak při tvorbě bezpečnostní dokumentace a přípravě havarijních plánů, tak i při provozu a rozvoji Vašeho IT. Poskytneme Vám nástroje pro správu bezpečnostní dokumentace, řízení aktiv a zavádění bezpečnostních opatření.

Oblasti bezpečnosti:
- **ISO 27k**
- **ISO 22301**
- **ISO 31000**
- **Zákon č. 181/2014 Sb.**
- **Zákon č. 253/2008 Sb.**
- **GDPR**

Funkcionality:
- Vlastní správa číselníků
- Volitelná struktura dat
- Nastavení pozadí položek
- Definice šablon dokumentace
- Vytváření vlastních sestav
- Nastavení vlastních vzorců
- Výpočty a hodnocení
- Dynamické animované grafy
- Filtrování, vyhledávání, export
- Obesílání týmu

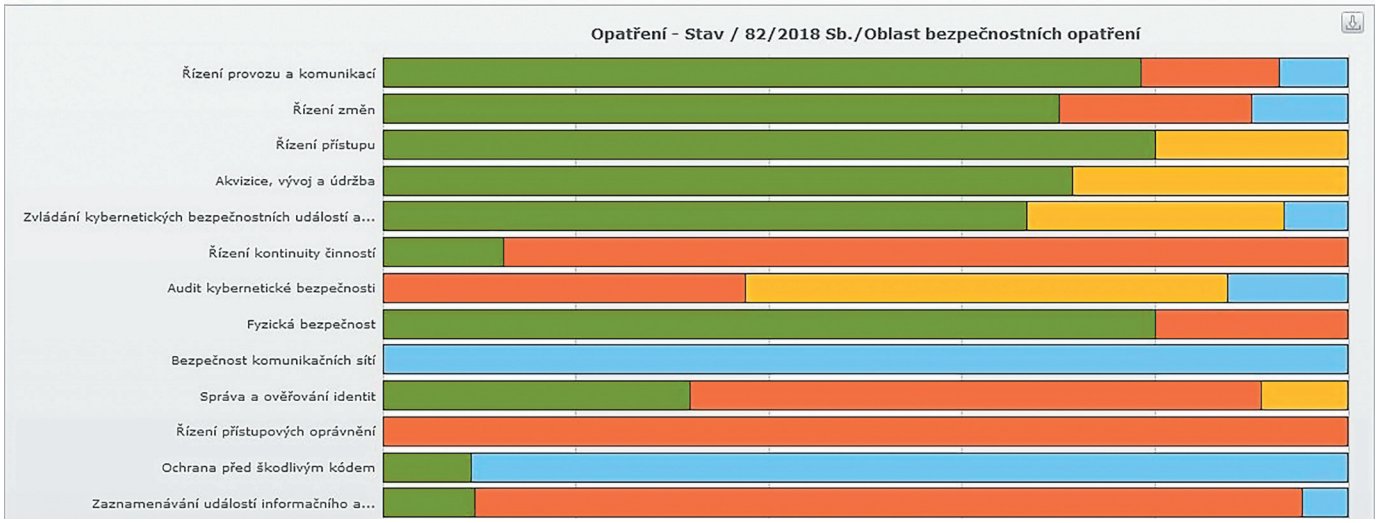
Šablony:
- Katalog aktiv
- Katalog hrozeb
- Prohlášení o aplikovatelnosti
- Analýza rizik
- Plán opatření
- Hodnocení souladu

Komplexní číselníky:
- ISO 27k
- Zákon č. 181/2014 Sb.
- GDPR GAP
- AML

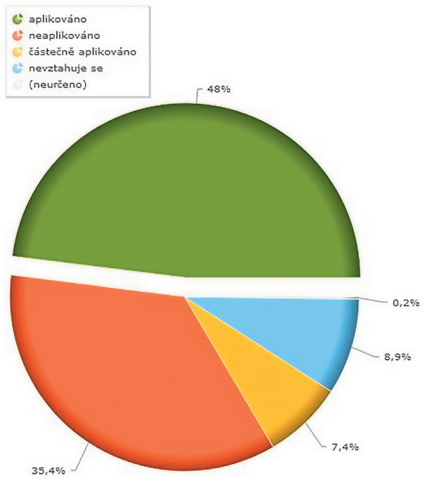
Individuální číselníky:
- Důvěrnost
- Priorita
- Stav
- Kategorie aktiva
- Dostupnost aktiva
- Integrita aktiva
- Hodnota aktiva
- Úroveň dopadu
- Způsob likvidace aktiva
- Důvod zpracování aktiva
- Rozsah zpracování aktiva
- Úroveň hrozby
- Úroveň zranitelnosti
- Úroveň rizika
- Druh hrozby
- Skupina zranitelnosti

PragoData a.s.
www.pragodata.com
Opletalova 1418/23, 110 00 Praha 1
info@pragodata.com

Opatření



	Bezpečnostní opatření	Stav	Odůvodnění / způsob implementace	Dokumentace
§ 3 a)	stanoví s ohledem na požadavky dotčených stran a organizační bezpečnost rozsah systému řízení bezpečnosti informací, ve kterém určí organizační části a aktiva, jichž se systém řízení bezpečnosti informací týká	aplikováno	Bezpečnostní politika	SM-BEZP-01
§ 3 b)	stanoví cíle systému řízení bezpečnosti informací	aplikováno	Bezpečnostní politika	SM-BEZP-01
§ 3 c)	pro stanovený rozsah systému řízení bezpečnosti informací na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a hodnocení rizik zavede přiměřená bezpečnostní opatření	částečně aplikováno	Probíhá redesign BP	
§ 3 d)	řídí rizika podle § 5	neaplikováno	Naplánováno vytvoření metodiky pro řízení rizik do 11/2018	ISO 31000
§ 3 e)	vytvoří a schválí bezpečnostní politiku v oblasti systému řízení bezpečnosti informací, která obsahuje hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací, a na základě bezpečnostních potřeb a výsledků hodnocení rizik stanoví bezpečnostní politiku v dalších oblastech podle § 30 a zavede přiměřená bezpečnostní opatření	částečně aplikováno	Probíhá redesign BP	
§ 3 f)	zajistí provedení auditu kybernetické bezpečnosti u informačního a komunikačního systému (dále jen „audit kybernetické bezpečnosti“) podle § 16	neaplikováno	Nebyl realizován, naplánován na 11/2018	
§ 3 g)	zajistí pravidelné vyhodnocování účinnosti systému řízení bezpečnosti informací, které obsahuje hodnocení stavu systému řízení bezpečnosti informací včetně revize hodnocení rizik, posouzení výsledků provedených auditů kybernetické bezpečnosti a dopadů kybernetických bezpečnostních incidentů na systém řízení bezpečnosti informací	neaplikováno	Neproběhlo, bude realizováno na základě 1. auditu organizace	
§ 3 h)	průběžně identifikuje a následně podle § 11 řídí významné změny, které patří do rozsahu systému řízení bezpečnosti informací	neaplikováno	Bude aktualizována Bezpečnostní politika	SM-BEZP-01



Aktivum	Riziko	Zranitelnost	Hrozba	Úr. dopadu	Úr. hrozby	Úr. zranitelnost	Úroveň rizika
Ekonomický systém (ERP)	R1	Známé chyby v programech	Zneužití oprávnění	Střední	Kritická	Kritická	Vysoké
LDAP	R2	Neprovádění logování událostí	Zneužití oprávnění	Vysoký	Vysoká	Vysoká	Vysoké
Osobní počítač	R3	Odcizení	Krádež zařízení	Střední	Nízká	Vysoká	Nízké
Nahrávací studio	R4	Odcizení	Krádež zařízení	Vysoký	Nízká	Kritická	Střední
Tiskárna Minolta TPKC	R5	Požár	Požár	Vysoký	Nízká	Nízká	Nízké
Datový portál	R6	Upgrade systému	Poškození dat	Vysoký			
Ekonomický systém (ERP)	R7	SW je již nepodporovaný - EOL	Chybné fungování aplikačního programového vybavení	Střední	Kritická	Střední	Střední
Kamerový systém	R8	Hrozí vandalismus a zneužití	Nezákonné zpracování dat	Střední	Vysoká	Střední	Střední

PragoData a.s.
www.pragodata.com
Opletalova 1418/23, 110 00 Praha 1
info@pragodata.com