ICZ RISK*GUIDE

HODNOCENÍ RIZIK

ICZ RISK*GUIDE JE IDEÁLNÍM NÁSTROJEM PRO SPRÁVU CELÉ AGENDY ŘÍZENÍ RIZIK A HODNOCENÍ AKTIV VE VAŠÍ ORGANIZACI. VÝRAZNĚ ZRYCHLUJE A USNADŇUJE PROCES HODNOCENÍ RIZIK I PLÁNOVANÍ A REALIZACI ADEKVÁTNÍCH NÁPRAVNÝCH OPATŘENÍ. ZÁROVEŇ JE PLNĚ V SOULADU S PLATNOU I CHYSTANOU LEGISLATIVOU NEJEN PRO OBLAST KYBERNETICKÉ BEZPEČNOSTI - NIS2.

KLÍČOVÉ PŘÍNOSY

- Komplexní správa rizik
- Kontinuita a sledování trendů v čase
- Integrované metodiky
- Katalog hrozeb a bezpečnostních opatření
- Modelování aktiv a jejich vazeb
- Modulární a otevřené řešení pro řízení různých rizik organizace (finanční, projektová)

Aplikace ICZ Risk*Guide je **univerzální nástroj pro hodnocení rizik** v rámci různých oblastí činnosti organizace.

Plná verze ICZ Risk*Guide zajistí hodnocení a analýzu rizik kybernetické bezpečnosti, správu bezpečnostních a nápravných opatření k eliminaci rizik, řízení rizik podle zákona o finanční kontrole a řízení projektových rizik. Modulární platforma je od počátku vyvíjena pro daný účel – hodnocení rizik organizace, což umožnilo důsledně kopírovat optimální průběh práce s riziky. Uživatel je systémem intuitivně veden procesem hodnocení rizik. Jednotlivé moduly lze pořizovat postupně podle potřeb.

VÝHODY

- Bezpapírové řešení hodnocení rizik
- Přehled o aktuálním stavu rizik
- Přehled o bezpečnostních opatřeních k eliminaci hrozeb na aktiva
- Detailní modelování a hodnocení aktiv
- Přehled o nápravných opatřeních
- Řízení přístupu a oprávnění
- Možnost AJ i jiných jazyků
- Rizika jsou dlouhodobě pod kontrolou
- Pro řízení kybernetické bezpečnosti i jiných oblastí organizace
- Podklad pro audity na jednom místě
- Modulární řešení
- Exporty výstupu

[ICZRISK*GUIDE]

Aplikace podporuje všechny etapy procesu analýzy rizik, což jsou identifikace, analýza a vyhodnocení rizik. Na základě vyhodnocení a kvantifikace rizik aplikace umožňuje vybrat bezpečnostní opatření pro snížení rizik a minimalizaci dopadů potenciálních hrozeb na aktiva.

Analýza rizik kybernetické bezpečnosti IT probíhá v těchto etapách:

- Stanovení kontextu analýzy rizik
- Stanovení hranice analýzy rizik, výběrem aktiv, která budou do analýzy zahrnuta
- Identifikace a seskupování aktiv a posuzování jejich hodnoty
- Identifikace hrozeb
- Identifikace stávajících opatření na ošetření hrozeb
- Identifikace zranitelnosti aktiv
- Identifikace dopadů a následků působení hrozeb na aktiva
- Analýza hrozeb a zranitelnosti aktiv
- Průběžné hodnocení rizik
- Ošetření rizik pomocí nových opatření a akceptace přijatelné míry rizika

[ZÁKLADNÍ VLASTNOSTI APLIKACE ICZ RISK*GUIDE]

Evidence akcí hodnocení rizik:

- Možnost výběru metodiky hodnocení rizik
- Nastavení kvalitativního hodnocení rizik
- Hierarchická evidence a ohodnocení aktiv
- Evidence a hodnocení hrozeb
- Výpočet inherentního a výchozího rizika
- Evidence a přiřazení opatření pro ošetření rizik
- Výpočet zbytkového rizika
- Evidence a hodnocení aktiv
- Vazby mezi primárními a podpůrnými aktivy
- Export nebo import katalogů hrozeb a opatření
- Kontextová nápověda
- Řízení přístupů a práv
- Notifikace
- Audit log, technické informace, administrace

Výstupy

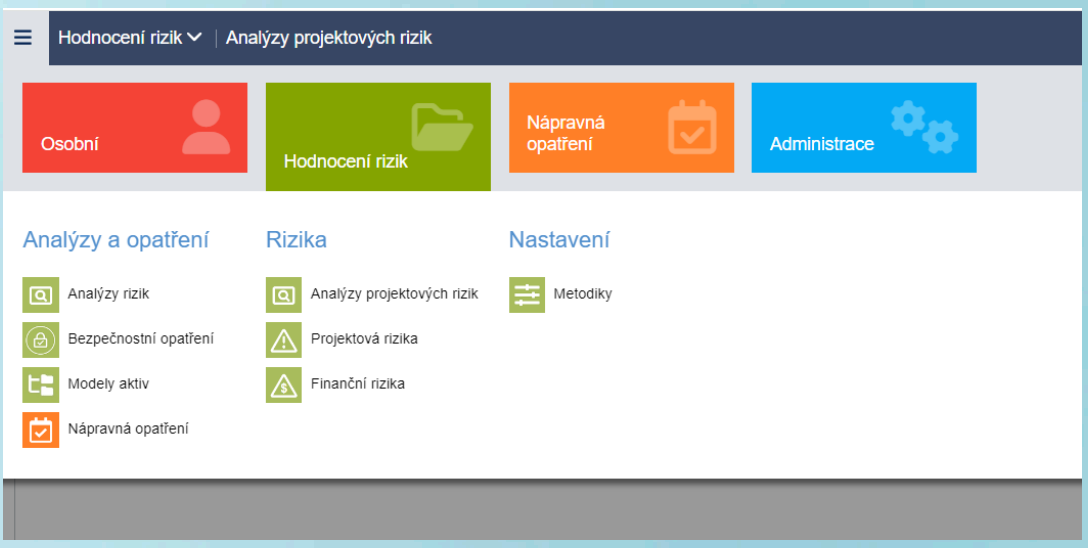
- Prohlášení o aplikovatelnosti, Plán zvládání rizik (kybernetická bezpečnost)
- Katalog rizik (finanční a projektová rizika)
- Grafické znázornění vazeb mezi aktivy (export pro účely prezentace)
- Export aktiv včetně vzájemných vazeb

[MODULÁRNÍ ŘEŠENÍ APLIKACE ICZ RISK*GUIDE]

Modulární platforma je od počátku vyvíjena pouze pro účely hodnocení rizik organizace, což se projevuje fokusem na komplexnost, zároveň však intuitivnost a ergonomii užívání v jakékoli oblasti, kde rizika potřebujete monitorovat.

Další moduly aplikace Risk*Guide jsou moduly pro rozšíření práce s nápravnými opatřeními a řízení dalších oblastí rizik organizace:

- sledování nápravných opatření ve vazbě na bezpečností opatření v rámci řízení rizik kybernetické bezpečnosti (modul Nápravná opatření)
- řízení rizik podle zákona o finanční kontrole (Modul Finanční rizika)
- řízení rizik v rámci přípravy a realizace projektů (Modul Projektová rizika)
- hodnocení aktiv a vytváření vazeb mezi nimi (Modul Modelování aktiv)



Nápravná opatření (NO)

Modul nápravných opatření ICZ Risk*Guide zajišťuje správu nápravných opatření a jejich řízení. Účelem je předcházení rizika. Modul nápravných opatření zahrnuje přípravu nápravného opatření a jeho schválení, realizaci, monitorování nápravného opatření a archivaci implementovaného opatření. Modul nápravných opatření je provázán na bezpečnostní opatření.

- Modul nápravných opatření umožňuje správu celého cyklu nápravných opatření.
- Umožňuje přiřazení NO a sledování plnění nápravných opatření (vlastník, termíny, stav).
- K nápravnému opatření je možné připojit tým, komentáře, sdílet je v týmu nebo emailem.
- Systém notifikací je možné využít na upozornění na termíny plnění a jiné události.

Modelování aktiv

Modul Modelování aktiv umožnuje identifikovat, evidovat a zpracovat „rodinné stříbro“ s dostatečným detailem a plně v souladu s dozorujícími orgány (NÚKIB).

- Evidence vyššího detailu aktiv bez zbytečného zvyšování složitosti hodnocení rizik
- Upřesnění způsobu přenosu hodnoty aktiv mezi primárními a podpůrnými aktivy
- Vytváření sdružených aktiv pro aktiva se stejnou charakteristikou
- Sledování dopadů konkrétních rizik nejen na sdružená a dílčí aktiva

Finanční rizika - řízení rizik podle zákona o finanční kontrole

Modul Finanční rizika slouží jako nástroj k evidenci a řízení rizik podle zákona o finanční kontrole (Zákon č. 320/2001 Sb.) a metodiky řízení rizik ve veřejné správě (MF ČR).

- V rámci veřejné správy jsou hlavními uživateli - útvar interního auditu a vedoucí odborů / oddělení
- Identifikace rizika, výpočet hodnoty rizika (dopad, pravděpodobnost), určení strategie k řízení rizika, určení vlastníka rizika a opatření k eliminaci rizika
- Karta rizika
- Role – zakladatel rizika, vlastník rizika, vlastník opatření
- Seznam rizik a opatření – export do xls formátu (Katalog rizik)
- Grafické znázornění podle úrovně a druhu rizika – export do formátu png, jpeg, svg

Projektová rizika - řízení projektových rizik

Modul Projektová rizika zajišťuje evidenci a řízení projektových rizik založené na metodice řízení rizik projektového řízení vycházející z Prince2 a IPMA.

- Projektová rizika jsou nutná řídit u všech připravovaných i realizovaných projektů
- V rámci veřejné správy jsou hlavními uživateli projektoví manažeři, útvary, které připravují veřejné zakázky a žádosti o dotace, vedoucí odborů dotčení realizací projektů
- Identifikace rizika, výpočet hodnoty rizika (dopad, pravděpodobnost), určení strategie k řízení rizika, určení vlastníka rizika a opatření k eliminaci rizika
- Karta rizika
- Role – zakladatel rizika, vlastník rizika, vlastník opatření
- Seznam rizik a opatření – export do xls formátu (Katalog rizik)
- Grafické znázornění podle úrovně a druhu rizika – export do formátu png, jpeg, svg

[VYUŽITÁ METODIKA]

Řízení rizik kybernetické bezpečnosti IT

V aplikaci byla implementována metodika hodnocení rizik podle mezinárodního standardu ISO/IEC 27005, která se týká bezpečnosti informačních systémů a bezpečnosti informací IT/ISMS. Použitá vodítka vychází z vyhlášky o kybernetické bezpečnosti (vyhláška č. 82/2018 Sb.) a dalších doporučení Národního úřadu pro kybernetickou a informační bezpečnost. Zvolená metodika je po úpravě nebo vytvoření nových katalogů hrozeb a opatření případně i metrik, použitelná i v dalších oblastech.

Metodika je kvalitativní, využívá stupnice typu nízký – střední – vysoký – kritický alias 1-2-3-4. Úroveň rizika je odhadována na základě třech dílčích ohodnocení – ohodnocení dopadu, ohodnocení hrozby a ohodnocení úrovně opatření (opaku zranitelnosti).

Aplikace též umožňuje využití metodiky ISO/IEC 27005 a na ní navázané české legislativy – zákon/vyhláška o kybernetické bezpečnosti.

Finanční rizika - řízení rizik podle zákona o finanční kontrole

Evidence a řízení rizik je připraven podle zákona o finanční kontrole (Zákon č. 320/2001 Sb.) a metodiky řízení rizik ve veřejné správě (MF ČR).

Projektová rizika - řízení projektových rizik

Evidence a řízení projektových rizik vychází z mezinárodních standardů a metodik projektového řízení Prince2 a IPMA.

[VARIANTY APLIKACE ICZ RISK*GUIDE]

Aplikace ICZ Risk*Guide se přizpůsobí potřebám Vaší organizace. Můžete zvolit variantu, která nejvíce odpovídá Vašim potřebám pro hodnocení a řízení rizik IT ve Vaší organizaci. Varianty se liší způsobem nasazení buď:

- přímo ve vaší organizaci
- prostřednictvím cloudové služby provozované ze zabezpečeného datového centra ICZ.

[DOPLŇKOVÉ SLUŽBY V OBLASTI METODIKY PRO HODNOCENÍ RIZIK IT]

Základní služby v oblasti metodiky pro hodnocení rizik IT

V rámci pořízení nástroje ICZ Risk*Guide každý zákazník dostane připravený **katalog hrozeb a bezpečnostních opatření (oblast kybernetické bezpečnosti IT)**, aby ihned mohl začít provádět hodnocení rizik svého informačního systému.

- Katalog hrozeb i katalog bezpečnostních opatření bude k dispozici
  - ve formě číselníku určeného pro import do nástroje,
  - dokumentu popisujícího jednotlivé hrozby nebo bezpečnostní opatření.
- U katalogu opatření si může zákazník vybrat jeden ze dvou připravených katalogů opatření, a to
  - katalog opatření vycházející ze struktury ČSN EN ISO/IEC 27002, nebo
  - katalog opatření vycházející ze struktury opatření uvedených ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti.

Nadstavbové služby v oblasti metodiky analýzy a hodnocení rizik ICT

V případě zájmu zákazníka je společnost ICZ připravena nabídnout další nadstavbové služby nad rámec základních služeb, a to zejména:

- Dodání standardizované metodiky hodnocení rizik, která bude obsahovat popis jednotlivých kroků provádění hodnocení a řízení rizik a vodítka pro určení hodnoty aktiv, hrozeb a úrovně opatření.
- Úpravu výše uvedené standardizované metodiky hodnocení rizik dle prostředí a požadavků zákazníka, a to zejména úpravu vodítek, katalogu hrozeb a opatření a procesu akceptace rizika dle potřeb zákazníka.
- Analýzu metodiky zákazníka a vypracování doporučení na její úpravu tak, aby zohledňovala logiku nástroje ICZ Risk*Guide.
- Provedení hodnocení rizik systému nebo prostředí zákazníka, tedy provedení celého hodnocení rizik dle dodané nebo upravené metodiky hodnocení rizik. Toto hodnocení rizik bude prováděno v nástroji ICZ Risk*Guide.
- Provedení rozdílové analýzy (GAP analýzy) stavu bezpečnostních opatření proti obecně uznávanému seznamu opatření, kterým je ČR standard ČSN EN ISO/IEC 27002, nebo vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti. Tuto rozdílovou analýzu je vhodné provést jako součást hodnocení rizik za účelem zmapování stavu bezpečnostních opatření, tak i po čase za účelem ověření stavu implementace nových opatření.

OBCHODNÍ KONTAKT

ICZ a.s. Na hřebenech II 1718/10
140 00 Praha 4
TEL: +420 222 271 111
E-MAIL: riskguide@i.cz

ICZ Risk*Guide