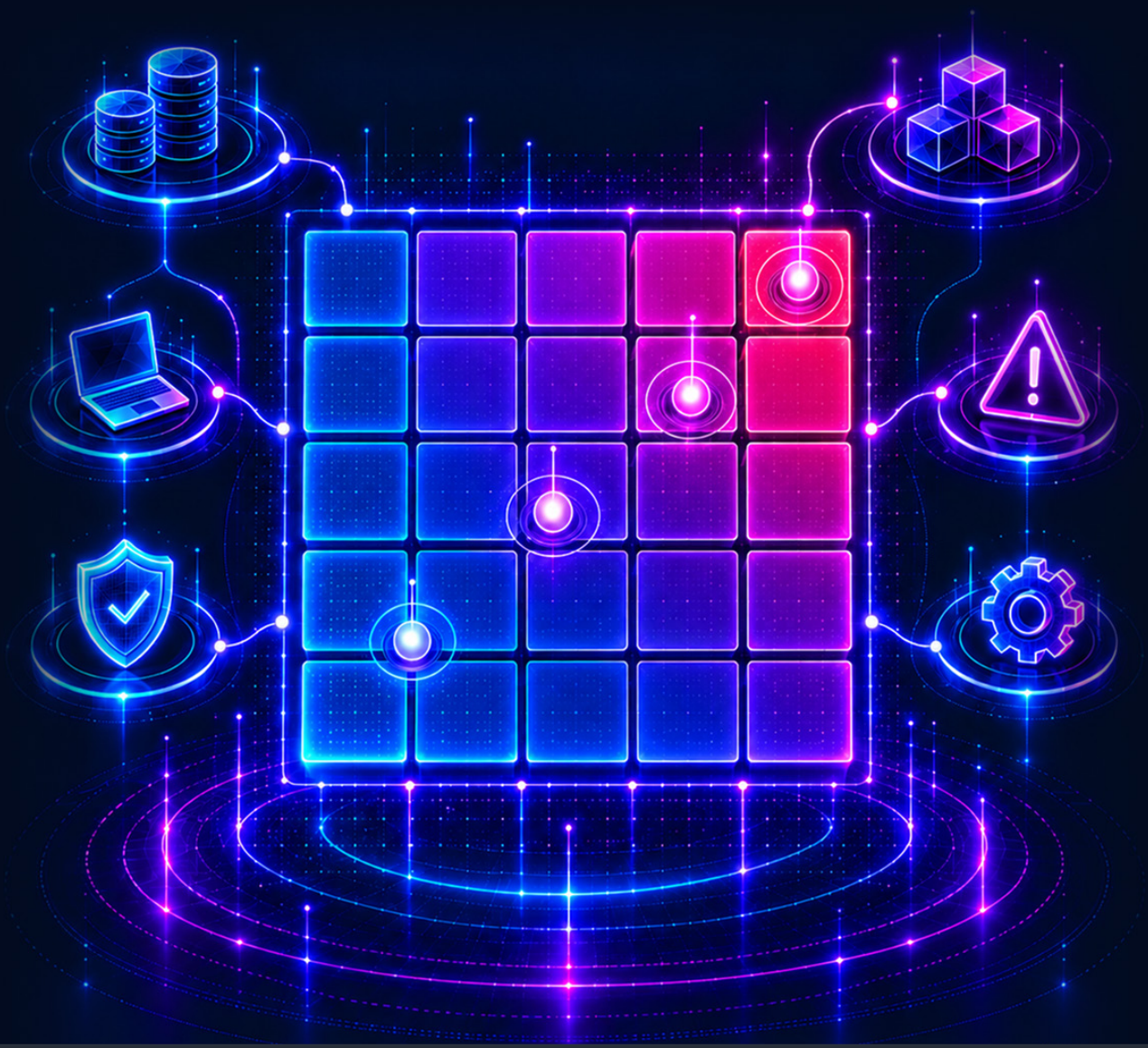
FREEDIVISION

SOLUTION GUIDE



FreeDivision.io Risk

Cyber Risk Management

Získejte přehled o aktivech, rizicích a bezpečnostních opatřeních v jednom prostředí – od evidence aktiv přes analýzu rizik až po kontrolu opatření, audity a dodavatele.

Bez znalosti aktiv není možné řídit riziko

Kybernetická bezpečnost není jen o technologiích. Organizace potřebuje vědět, co je pro ni důležité, jaká rizika jí hrozí, jaký mohou mít dopad a jakými opatřeními je dokáže řídit.

Každá organizace má desítky nebo stovky aktiv – aplikace, servery, informační systémy, procesy, data, dodavatele i služby. Jsou vzájemně propojená, mají různou hodnotu a jsou vystavena různým hrozbám.

Problém nastává ve chvíli, kdy organizace jednotlivé informace eviduje odděleně: aktiva v tabulce, rizika v Excelu, audit v dokumentu bez auditních stop a opatření v seznamu bez role managementu. Výsledkem je roztříštěnost informací, komplikovaná spolupráce a vyšší chybovost.

Bez jednotného a kontinuálního procesu je navíc obtížné udržovat data aktuální a efektivně zapojit gestory aktiv do řízení rizik.

FreeDivision.io Risk je postaven na opačném principu. Propojuje aktiva, vazby, hrozby, zranitelnosti, rizika, opatření i jejich kontrolu. Nevzniká tak pouze evidence aktiv nebo seznam rizik – organizace získává kontext, který umožňuje jednotlivá rizika skutečně řídit.

Executive Summary

FreeDivision.io Risk propojuje správu aktiv, identifikaci hrozeb, rizik a zranitelností, řízení bezpečnostních opatření, audity i správu dodavatelů do jednoho prostředí. Výsledkem je ucelený pohled na bezpečnostní rizika organizace, jejich analýzu a vývoj v čase.

Řešení podporuje celý proces Identifikace · Analýza · Hodnocení · Náprava · Kontrola. Vizualizuje vazby mezi aktivy, převádí hrozby a zranitelnosti do srozumitelného hodnocení rizika, řídí plán zvládání rizik a průběžně ukazuje, zda přijatá opatření riziko skutečně snižují. Pokrývá také audity, řízení dodavatelů a Business Continuity Management.

Řešení je postaveno na metodice NÚKIB a normě ISO 27000, lze je rozšířit o DORA nebo NIS2 a vzniká v České republice v souladu s evropskou legislativou. Cílem je kontinuální proces řízení rizik, nikoli jednorázový risk assessment.



Poznejte svá aktiva. Identifikujte rizika.
Nastavte opatření. Sledujte výsledek.

Jak řešení funguje

FreeDivision.io Risk vede organizaci od aktiv až ke kontrole opatření. Každý krok navazuje na předchozí a všechny pracují se stejným kontextem – aktivy, jejich vazbami, hrozbami, riziky a opatřeními.

Řízení rizik tak není jednorázové vyplnění tabulky, ale průběžný proces, který reaguje na nová aktiva, změny dodavatelů, nové hrozby i měnící se regulatorní požadavky.

Poznat aktiva

Evidence aktiv organizace s jejich významem, hodnotou a vlastníkem – data, informační systémy a aplikace, servery a infrastruktura, procesy a služby, dodavatelé i zaměstnanci a organizační jednotky.

Výsledkem je jednotný přehled o tom, co organizace vlastní a co potřebuje chránit.

Pochopit vazby

Výpadek nebo kompromitace jednoho systému může mít dopad na další služby, procesy nebo infrastrukturu. Vazby lze evidovat a zobrazit tabulkově i graficky v mapě aktiv.

Je tak vidět, která aktiva jsou kritická, na čem závisí, jak se může riziko šířit a kde může mít incident největší dopad.

Vyhodnotit riziko

Hrozby a zranitelnosti se hodnotí v kontextu konkrétních aktiv. Otázkou není jen „Jaké máme zranitelnosti?“, ale „Jaké riziko představuje konkrétní zranitelnost nebo hrozba pro konkrétní aktivum?“

Z hodnoty aktiva, hrozeb, zranitelností a pravděpodobnosti dopadu vzniká celková úroveň rizika – a s ní jasná priorita.

Naplánovat zvládání

Identifikace rizika sama o sobě bezpečnost nezlepší. Plán zvládání rizik určuje opatření s odpovědnou osobou, termínem, stavem, prioritou, souvisejícím rizikem a dokumentací.

K dispozici je katalog oblastí dopadu podle vyhlášky č. 409/2025 Sb.

Kontinuální kontrola

Riziko → Opatření → Stav → Výsledek. Organizace průběžně kontroluje, zda přijatá opatření skutečně vedou ke snížení rizika. Opakované činnosti – například formuláře pro hodnocení dodavatelů, pravidelné kontroly nebo jednotlivé kroky bezpečnostních a compliance procesů lze automatizovat podle předem definovaných pravidel a přizpůsobit požadavkům organizace.

Klíčové schopnosti řešení

Jeden systém pro bezpečnostní agendy, které bývají rozdělené mezi několik nástrojů, tabulek a dokumentů.

Aktiva a mapa vazeb

Přehled aktiv s řazením, filtrováním a zakládáním nových záznamů. Závislosti mezi aktivy lze zobrazit v grafu vazeb včetně navázaných hodnocení rizik. Vizualizace vazeb je jedním z prvků, kterými se řešení odlišuje od většiny nástrojů na trhu.

Analýza a zvládání rizik

Hodnocení rizika s vazbou na zranitelnosti, hrozby a odpovědné osoby, včetně hodnocení dostupnosti, ztráty důvěry a integrity. Plán zvládání rizik s opatřeními, termíny a odpovědnostmi a sledování jejich vývoje v čase.

Audity

Evidence, plánování a správa auditů včetně auditních zpráv s jednotlivými verzemi, datem, typem zprávy a přílohou. Auditní zprávy lze generovat automaticky a zjištění propojit s riziky a opatřeními.

Dodavatelé a kontinuita

Evidence a hodnocení dodavatelů z pohledu jejich bezpečnostního rizika a propojení s aktivy a riziky. Podpora Business Continuity Managementu (BCM) a tvorby Business Continuity Planu (BCP).

Metodika a provoz

FreeDivision.io Risk vychází z ověřených metodik a přizpůsobí se prostředí organizace – metodicky i technicky.

[METODIKA]

Postaveno na metodice NÚKIB a normě ISO 27000

Řešení je postaveno na principech metodiky NÚKIB a normy ISO 27000. Současně je lze rozšířit o další metodiky, například DORA nebo NIS2.

Protože se implementace NIS2 v jednotlivých členských státech EU liší, lze metodiky individuálně přizpůsobit regionálním požadavkům.

[PROVOZ]

Online i on-premise, s integrací do ekosystému

Řešení lze provozovat online i on-premise. Obsahuje integrovaný DMS a reporting a integruje se s Identity Managementem, SIEM a dalšími nástroji.

V rámci implementační analýzy identifikujeme místa vhodná pro automatizaci a jednotlivé procesy i pracovní postupy přizpůsobíme konkrétním požadavkům organizace.

Typické scénáře využití

FreeDivision.io Risk pomáhá organizaci zjistit, co má, co ji ohrožuje a zda přijatá opatření skutečně fungují.

Od Excelu k řízení rizika

Duplicitní tabulky a samostatně vedené seznamy nahrazuje jedno prostředí, ve kterém lze sledovat celý životní cyklus rizika:
Aktiva → Rizika → Opatření → Audity → Kontrola.

Data zůstávají aktuální a gestoři aktiv se mohou efektivně zapojit do řízení rizik.

Audit, který nekončí v archivu

Bezpečnostní audit často končí dokumentem, který se po několika týdnech stane pouze archivním záznamem.

FreeDivision.io Risk propojuje audit s řízením rizik:
Audit → Zjištění → Riziko → Opatření → Kontrola.

Rizika dodavatelského řetězce

Externí IT služby, cloudové platformy, poskytovatelé technologií nebo další partneři mohou mít přístup ke kritickým systémům a datům.

Dodavatele lze evidovat, hodnotit, sledovat jejich stav a dokumentaci a propojit je s aktivy a riziky.

Výpadek kritické služby

„Co se stane, když dojde k výpadku kritické služby?“

A následně:
„Jak zajistíme její obnovu?“

Podpora BCM a BCP propojuje řízení kybernetických rizik s dostupností klíčových služeb organizace.

Přínosy pro organizaci

Hodnotou FreeDivision.io Risk není další evidence, ale rizika, která jsou průběžně pod kontrolou.



Ucelený přehled o rizicích

Všechny důležité informace o aktivech, rizicích a opatřeních máte vždy po ruce – v jednom prostředí.



Lepší prioritizace

Zaměříte se nejdříve na rizika, která mohou mít největší dopad. Méně kritická rizika lze řešit později.



Připravenost na audit

Potřebnou dokumentaci, historii a auditní výstupy máte na jednom místě.



Podpora regulatorních požadavků

Strukturované řízení rizik pomáhá pracovat s požadavky bezpečnostních standardů a regulace.

Řídíme rizika všech aktiv

FreeDivision.io Risk eviduje aktiva organizace a pracuje s jejich významem, hodnotou a vzájemnými vztahy.

Procesy a služby

Business úroveň – co organizace skutečně dodává. Zde se řízení rizik propojuje s BCM.

Dodavatelé

Externí aktiva mimo přímou kontrolu, často s přístupem k systémům a datům organizace.

Zaměstnanci a jednotky

Určují vlastníky a gestory aktiv. Bez jasného přiřazení se rizika obtížně řídí i eskalují.

Data

Nejcennější a nejcitlivější aktivum – primární cíl útoků. Určuje, jak přísně chránit vše, co s daty pracuje.

Systémy a aplikace

Zpracovávají a zpřístupňují data. Kompromitace ohrožuje jejich důvěrnost, integritu i dostupnost.

Servery a infrastruktura

Technický základ systémů. Zranitelnost v síti, na serverech nebo v cloudu může ohrozit více systémů naráz.

Podporované metodiky a regulace

NÚKIB · ZoKB · Vyhláška č. 409/2025 Sb. · NIS2 · DORA · ISO 27000 · ISO 31000 · BCM / BCP

Provoz a integrace

Online · On-premise · Integrovaný DMS · Reporting · Workflow · Identity Management · SIEM · Další nástroje

Připraveno na regulaci

Strukturované řízení rizik pomáhá pracovat s požadavky bezpečnostních standardů a regulace a mít potřebnou dokumentaci na jednom místě.

NIS2

Směrnice EU o kybernetické bezpečnosti

ZoKB

Zákon o kybernetické bezpečnosti (NÚKIB)

DORA

Odolnost finančních institucí

ISO 27000

Bezpečnost informací a řízení rizik

Odpovědi na zásadní otázky

FreeDivision.io Risk pomáhá organizaci odpovědět na otázky, které si klade vedení, bezpečnost, gestoři aktiv i auditoři.

Co máme?

Jednotná evidence aktiv, jejich hodnoty a vlastníků.

Co je pro nás kritické?

Mapa vazeb ukáže, na čem závisí klíčové služby.

Co nás může ohrozit?

Hrozby a zranitelnosti v kontextu konkrétních aktiv.

Jak velké je naše riziko?

Pravděpodobnost, dopad a celková úroveň rizika.

Co s ním děláme?

Plán zvládání rizik s konkrétními opatřeními.

Kdo je za opatření odpovědný?

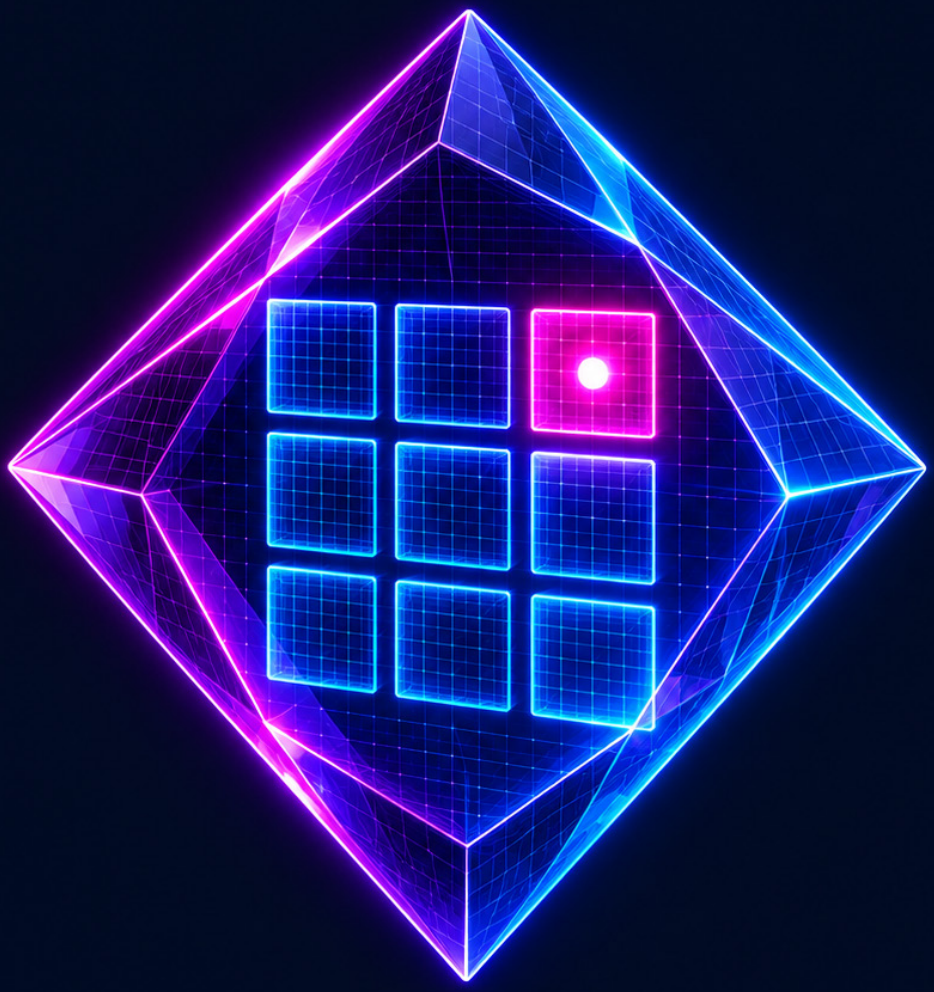
Odpovědná osoba, termín a stav u každého opatření.

Snižuje se naše riziko?

Stav rizik a opatření sledovaný v čase.

Jsme schopni svůj stav doložit?

Dokumentace, historie a auditní výstupy na jednom místě.



Proč FreeDivision

Úspěšná kybernetická bezpečnost nestojí pouze na moderních technologiích. Stejně důležití jsou lidé, správně nastavené procesy a schopnost dlouhodobě udržet rizika pod kontrolou.

Proto stavíme všechna řešení platformy FreeDivision.io na třech vzájemně propojených pilířích.

Technologie

FreeDivision.io Risk využívá specializovanou platformu pro řízení kybernetické bezpečnosti, aktiv, rizik, auditů a dodavatelů. Poskytuje centrální prostředí pro evidenci, hodnocení, workflow, reporting a dokumentaci.

Lze ji provozovat online i on-premise, obsahuje integrovaný DMS a reporting a integruje se s Identity Managementem, SIEM a dalšími nástroji.

Experti

Za řízením rizik nestojí jen nástroj, ale také lidé, kteří rozumí metodice i fungování organizace.

V rámci implementační analýzy specialisté FreeDivision identifikují místa vhodná pro automatizaci a přizpůsobí metodiku, procesy a pracovní postupy konkrétním požadavkům organizace.

Procesy

Řízení rizik přináší výsledky pouze tehdy, pokud je součástí pravidelného a systematického procesu. FreeDivision.io Risk podporuje celý cyklus Identifikace → Analýza → Hodnocení → Náprava → Kontrola. Automatizace omezuje manuální práci, snižuje riziko lidské chyby a zajišťuje, že se opakované činnosti provádějí konzistentně a podle předem definovaných pravidel. Cílem je kontinuální proces řízení rizik, nikoli jednorázový risk assessment.

FreeDivision.io jako platforma pro komplexní kybernetickou bezpečnost

FreeDivision.io Risk je součástí platformy FreeDivision.io, která propojuje technologie, odborné služby a řízení bezpečnosti do jednoho ekosystému.

Risk management dává největší smysl tehdy, když není izolovaný od ostatních bezpečnostních oblastí. Identifikované riziko lze přímo navázat na konkrétní technické opatření – řízení rizik se tak nezastavuje u dokumentace, ale reálně se propojuje s implementací opatření.

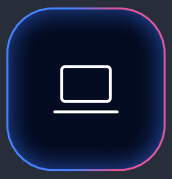
Řešení vzniká v České republice a jeho vývoj reflektuje aktuální požadavky evropské legislativy i specifika domácího prostředí.

Co nejlépe doplňuje FreeDivision.io Risk



Ochrana citlivých dat

FreeDivision.io Data chrání citlivá data a přístupová práva. Data jsou nejcennějším aktivem organizace – a tím i klíčovým vstupem pro hodnocení rizik.



Ochrana koncových zařízení

FreeDivision.io Essential zajišťuje detekci hrozeb a reakci na koncových zařízeních – konkrétní technické opatření, na které lze navázat identifikovaná rizika.



Správa zranitelností

FreeDivision.io Endpoint řeší správu zranitelností a patch management na koncových bodech – nápravu zranitelností, které Risk vyhodnocuje v kontextu aktiv.



Řízení bezpečnostních operací

FreeDivision.io Advanced propojuje bezpečnostní data a procesy do jednotného prostředí pro řízení bezpečnostních operací v rámci řešení SIEM/SOAR.



Threat Intelligence

FreeDivision.io CTI přináší proaktivní Cyber Threat Intelligence – přehled o vnějších hrozbách, které mohou organizaci a její aktiva ohrožovat.



Lidský faktor

FreeDivision.io PhishingGym systematicky snižuje lidské riziko prostřednictvím phishingových simulací a vzdělávání.



For Safety Reasons.
Be Best. Not First.

Závěr

Kybernetická bezpečnost není jen o technologiích. Organizace potřebuje vědět, co má, co je pro ni kritické, co ji může ohrozit a zda přijatá opatření skutečně fungují.

FreeDivision.io Risk propojuje aktiva, vazby, hrozby, rizika, opatření, audity i dodavatele do jednoho prostředí a umožňuje sledovat celý životní cyklus bezpečnostního rizika – od identifikace až po kontrolu výsledku.

Ve spojení s dalšími řešeními FreeDivision.io se řízení rizik nezastavuje u dokumentace, ale propojuje se s konkrétními technickými opatřeními. Řízení rizik bez slepých míst.

Efektivní řízení rizik snižuje náklady na bezpečnost

Domluvte si ukázku a uvidíte, jak FreeDivision.io Risk pomůže řídit rizika ve vaší organizaci. Poznejte svá aktiva. Identifikujte rizika. Nastavte opatření. Sledujte výsledek.

ADRESA

FreeDivision s.r.o.
Rektorská 50/52
108 00 Praha 10 – Malešice
Česká republika

KONTAKT

sales@freedivision.com
+420 220 972 426

www.freedivision.io