KATALÓG SLUŽIEB 2024

NAKIB

SOFTWAROVÉ VYBAVENIE

NÁRODNÁ AKADÉMIA PRE KYBERNETICKÚ
A INFORMAČNÚ BEZPEČNOSŤ

NAKIB.SK

NAKIB

SOFTWAROVÉ VYBAVENIE

Software pre Analýzu rizík ICT

Software pre Analýzu rizík privacy

Software pre riadenie štandardu TISAX

Riadenie Biznis Kontinuity

Software pre Analýzu rizík, Protikorupčný systém

NAKIB.SK

APLIKÁCIA NA VYKONÁVANIE ANALÝZY RIZÍK INFORMAČNEJ A KYBER BEZPEČNOSTI ZALOŽENÁ NA MEDZINÁRODNOM ŠTANDARDE ISO 27005 A KOMPATIBILNÁ S POŽIADAVKAMI NBU NA VÝKON RIADENIA RIZÍK.

Čo je?

Softvér SW pre analýzu rizík ICT je nástroj, ktorý umožňuje organizáciám identifikovať, analyzovať a hodnotiť riziká súvisiace s informačnými a komunikačnými technológiami (ICT). Softvér obsahuje nasledovné funkcie: Identifikácia rizík a zraniteľností: Pomáha pri identifikácii rôznych typov ICT rizík, ako napríklad technické riziká, operačné riziká, regulačné riziká, reputačné riziká a podobne. Analýza rizík: Umožňuje analyzovať identifikované riziká a zhodnotiť ich pravdepodobnosť a dopad na organizáciu. Hodnotenie rizík: Poskytuje nástroje na hodnotenie rizík a ich kategorizáciu podľa závažnosti. Plánovanie a implementácia kontrol: Umožňuje definovať a implementovať kontrolné mechanizmy na zníženie identifikovaných rizík. Monitorovanie a reporting: Poskytuje nástroje na monitorovanie rizík a reporting o stave a vývoji rizík. Obsahuje generovanie formulárov karty rizika a prijatie rizika manažmentom.

Prečo?

Zavedenie softvéru SW pre analýzu rizík ICT prináša viacero benefitov:
Zvýšenie informovanosti: Získanie komplexného prehľadu o ICT rizikách a ich dopade na organizáciu. Zníženie rizík: Predchádzanie ICT incidentom a minimalizácia ich dopadu na prevádzku a reputáciu organizácie. Zlepšenie riadenia ICT: Posilnenie riadenia ICT rizík a efektívnejšie alokovanie zdrojov na ich zníženie.Dodržiavanie regulácií: Zabezpečenie súladu s regulačnými požiadavkami na riadenie ICT rizík. Zvýšenie efektivity: Zníženie administratívnej záťaže a optimalizácia procesov riadenia ICT rizík.

Pre koho?

SW pre analýzu rizík ICT je určený pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za riadenie ICT rizík v rámci svojej organizačnej jednotky.
IT profesionálov: Ktorí sa podieľajú na identifikácii, analýze a hodnotení ICT rizík.
Audítorov: Ktorí sa venujú auditu ICT rizík a kontrol.
Konzultantov: Ktorí poskytujú poradenstvo v oblasti riadenia ICT rizík.
Každý, kto sa chce dozvedieť viac o analýze a riadení ICT rizík.

Prínosy?

Implementácia softvéru SW pre analýzu rizík PRIVACY prináša nasledovné prínosy:
Zvýšenie informovanosti o PRIVACY rizikách: Softvér umožňuje komplexnú identifikáciu a analýzu PRIVACY rizík a poskytuje prehľad o ich stave a vývoji. Zlepšenie riadenia PRIVACY: Softvér podporuje efektívne riadenie PRIVACY rizík a umožňuje definovanie a implementáciu vhodných kontrolných mechanizmov. Zníženie nákladov: Predchádzanie incidentom s únikom a zneužitím osobných údajov a minimalizácia ich dopadu môže priniesť značné úspory nákladov. Zvýšenie dôvery a reputácie: Demonštrovanie záväzku k ochrane osobných údajov posilňuje dôveru klientov, partnerov a regulačných orgánov. Zlepšenie strategického plánovania: Informácie o PRIVACY rizikách sú dôležitým vstupom pre strategické plánovanie a rozvoj organizácie.

APLIKÁCIA NA VYKONÁVANIE PRIVACY ANALÝZY RIZÍK ZALOŽENÁ NA MEDZINÁRODNOM ŠTANDARDE ISO 27005 A POŽIADAVKÁCH GDPR. JE APLIKOVANÝ PRIVACY ŠTANDARD ISO 29100

Čo je?

Softvér SW pre Analýzu rizík PRIVACY - Čo to znamená?
Softvér SW pre analýzu rizík PRIVACY je nástroj, ktorý umožňuje organizáciám identifikovať, analyzovať a hodnotiť riziká súvisiace s ochranou osobných údajov (PRIVACY). Softvér môže mať rôzne funkcie, ako napríklad: Identifikácia rizík: Pomáha pri identifikácii rôznych typov PRIVACY rizík, ako napríklad úniky osobných údajov, zneužitie osobných údajov, porušenie GDPR a podobne.
Analýza rizík: Umožňuje analyzovať identifikované PRIVACY riziká a zhodnotiť ich pravdepodobnosť a dopad na organizáciu. Hodnotenie rizík: Poskytuje nástroje na hodnotenie PRIVACY rizík a ich kategorizáciu podľa závažnosti. Plánovanie a implementácia kontrol: Umožňuje definovať a implementovať kontrolné mechanizmy na zníženie identifikovaných PRIVACY rizík. Monitorovanie a reporting: Poskytuje nástroje na monitorovanie PRIVACY rizík a reporting o stave a vývoji PRIVACY rizík.

Prečo?

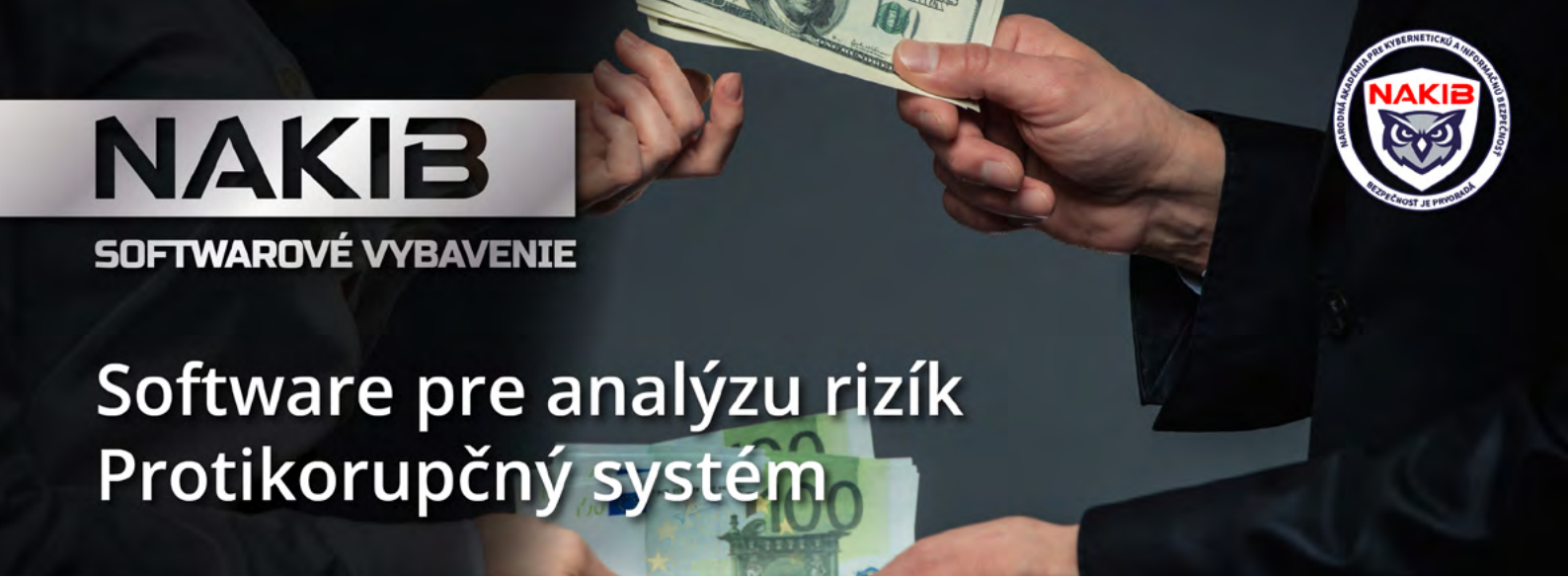
Zavedenie softvéru SW pre analýzu rizík PRIVACY prináša viacero benefitov:
Zvýšenie informovanosti: Získanie komplexného prehľadu o PRIVACY rizikách a ich dopade na organizáciu. Zníženie rizík: Predchádzanie incidentom s únikom a zneužitím osobných údajov a minimalizácia ich dopadu na prevádzku a reputáciu organizácie. Zlepšenie riadenia PRIVACY: Posilnenie riadenia PRIVACY rizík a efektívnejšie alokovanie zdrojov na ich zníženie. Dodržiavanie regulácií: Zabezpečenie súladu s regulačnými požiadavkami na ochranu osobných údajov, ako napríklad GDPR. Zvýšenie efektivity: Zníženie administratívnej záťaže a optimalizácia procesov riadenia PRIVACY rizík.

Pre koho?

Softvér SW pre analýzu rizík PRIVACY je určený pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za ochranu osobných údajov v rámci svojej organizačnej jednotky. IT profesionálov: Ktorí sa podieľajú na identifikácii, analýze a hodnotení PRIVACY rizík.
Audítorov: Ktorí sa venujú auditu ochrany osobných údajov. Konzultantov: Ktorí poskytujú poradenstvo v oblasti ochrany osobných údajov. Každý, kto sa chce dozvedieť viac o analýze a riadení PRIVACY rizík.

Prínosy?

Implementácia softvéru SW pre analýzu rizík PRIVACY prináša nasledovné prínosy:
Zvýšenie informovanosti o PRIVACY rizikách: Softvér umožňuje komplexnú identifikáciu a analýzu PRIVACY rizík a poskytuje prehľad o ich stave a vývoji. Zlepšenie riadenia PRIVACY: Softvér podporuje efektívne riadenie PRIVACY rizík a umožňuje definovanie a implementáciu vhodných kontrolných mechanizmov. Zníženie nákladov: Predchádzanie incidentom s únikom a zneužitím osobných údajov a minimalizácia ich dopadu môže priniesť značné úspory nákladov. Zvýšenie dôvery a reputácie: Demonštrovanie záväzku k ochrane osobných údajov posilňuje dôveru klientov, partnerov a regulačných orgánov. Zlepšenie strategického plánovania: Informácie o PRIVACY rizikách sú dôležitým vstupom pre strategické plánovanie a rozvoj organizácie.



NAKIB

SOFTWAROVÉ VYBAVENIE

Software pre analýzu rizík Protikorupčný systém

APLIKÁCIA NA VYKONÁVANIE PROTIKORUPČNEJ ANALÝZY RIZÍK ZALOŽENÁ NA MEDZINÁRODNOM ŠTANDARDE ISO 27005 A POŽIADAVKÁCH GDPR. JE APLIKOVANÝ ŠTANDARD ISO 37001.

Čo je?

Softvér SW pre analýzu rizík Protikorupčný systém je nástroj, ktorý umožňuje organizáciám identifikovať, analyzovať a hodnotiť riziká súvisiace s korupciou. Softvér môže mať rôzne funkcie, ako napríklad: Identifikácia rizík: Pomáha pri identifikácii rôznych typov korupčných rizík, ako napríklad podplácanie, úplatky, konflikty záujmov, zneužitie moci a podobne. Analýza rizík: Umožňuje analyzovať identifikované korupčné riziká a zhodnotiť ich pravdepodobnosť a dopad na organizáciu. Hodnotenie rizík: Poskytuje nástroje na hodnotenie korupčných rizík a ich kategorizáciu podľa závažnosti. Plánovanie a implementácia kontrol: Umožňuje definovať a implementovať kontrolné mechanizmy na zníženie identifikovaných korupčných rizík. Monitorovanie a reporting: Poskytuje nástroje na monitorovanie korupčných rizík a reporting o stave a vývoji korupčných rizík.

Prečo?

Zavedenie softvéru SW pre analýzu rizík Protikorupčný systém prináša viacero benefitov:
Zvýšenie informovanosti: Získanie komplexného prehľadu o korupčných rizikách a ich dopade na organizáciu. Zníženie rizík: Predchádzanie korupčným incidentom a minimalizácia ich dopadu na prevádzku a reputáciu organizácie. Zlepšenie riadenia protikorupčných opatrení: Posilnenie riadenia korupčných rizík a efektívnejšie alokovanie zdrojov na ich zníženie. Dodržiavanie regulácií: Zabezpečenie súladu s regulačnými požiadavkami na protikorupčné opatrenia. Zvýšenie efektivity: Zníženie administratívnej záťaže a optimalizácia procesov riadenia korupčných rizík.

Pre koho?

Softvér SW pre analýzu rizík Protikorupčný systém je určený pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za protikorupčné opatrenia v rámci svojej organizačnej jednotky. IT profesionálov: Ktorí sa podieľajú na identifikácii, analýze a hodnotení korupčných rizík.
Audítorov: Ktorí sa venujú auditu protikorupčných opatrení. Konzultantov: Ktorí poskytujú poradenstvo v oblasti protikorupčných opatrení. Každý, kto sa chce dozvedieť viac o analýze a riadení korupčných rizík.

Prínosy?

Implementácia softvéru SW pre analýzu rizík Protikorupčný systém prináša nasledovné prínosy:
Zvýšenie informovanosti o korupčných rizikách: Softvér umožňuje komplexnú identifikáciu a analýzu korupčných rizík a poskytuje prehľad o ich stave a vývoji. Zlepšenie riadenia protikorupčných opatrení: Softvér podporuje efektívne riadenie korupčných rizík a umožňuje definovanie a implementáciu vhodných kontrolných mechanizmov. Zníženie nákladov: Predchádzanie korupčným incidentom a minimalizácia ich dopadu môže priniesť značné úspory nákladov. Zvýšenie dôvery a reputácie: Demonštrovanie záväzku k protikorupčným opatreniam posilňuje dôveru klientov, partnerov a regulačných orgánov. Zlepšenie strategického plánovania: Informácie o korupčných rizikách sú dôležitým vstupom pre strategické plánovanie a rozvoj organizácie.

NAKIB

SOFTWAROVÉ VYBAVENIE

Software pre riadenie štandardu TISAX®

APLIKÁCIA NA PODPORU RIADENIE BEZPEČNOSTI TISAX® V ROZSAHU RIADENIA ZRELOSTI OPATRENÍ (SOA), ANALÝZY RIZÍK, RIADENIA TRETÍCH STRÁN A BCM A VÝKON INTERNÉHO AUDITU. APLIKÁCIA JE VYVINUTÁ NA TISAX® VER.06

Čo je?

SW pre riadenie štandardu TISAX® je nástroj, ktorý umožňuje organizáciám v automobilovom priemysle implementovať a udržiavať súlad s požiadavkami štandardu TISAX® (Trusted Information Security Assessment Exchange). Softvér môže mať rôzne funkcie, ako napríklad:
Riadenie požiadaviek: Umožňuje definovať, monitorovať a riadiť požiadavky štandardu TISAX®.
Hodnotenie rizík: Poskytuje nástroje na hodnotenie informačných bezpečnostných rizík v súlade s TISAX®.
Plánovanie a implementácia kontrol: Umožňuje definovať a implementovať kontrolné mechanizmy na zníženie identifikovaných rizík. Monitorovanie a reporting: Poskytuje nástroje na monitorovanie stavu informačnej bezpečnosti a reporting o súlade s TISAX®. Auditovanie: Umožňuje interný a externý audit súladu s požiadavkami TISAX®.

Prečo?

Zavedenie softvéru SW pre riadenie štandardu TISAX® prináša viacero benefitov:
Zvýšenie informačnej bezpečnosti: Zníženie rizika kybernetických útokov a ochranu citlivých informácií.
Zvýšenie dôvery a reputácie: Preukázanie záväzku k informačnej bezpečnosti a posilnenie dôvery partnerov a zákazníkov. Zjednodušenie auditov: Uľahčenie interných a externých auditov súladu s TISAX®.
Zníženie nákladov: Zníženie nákladov na riešenie kybernetických incidentov a sankcií za nesúlad s TISAX®.
Zlepšenie efektivity: Zníženie administratívnej záťaže a optimalizácia procesov riadenia informačnej bezpečnosti.

Pre koho?

SW pre riadenie štandardu TISAX je určený pre:
Výrobcov automobilov: Ktorí potrebujú preukázať súlad s TISAX® a chrániť svoje informačné systémy a dáta.
Dodávateľov automobilového priemyslu: Ktorí potrebujú spĺňať požiadavky TISAX® v rámci dodávateľského reťazca. IT profesionálov: Ktorí sa podieľajú na implementácii a udržiavaní súladu s TISAX®.
Audítorov: Ktorí sa venujú auditu informačnej bezpečnosti a súladu s TISAX®.
Každý, kto sa chce dozvedieť viac o štandarde TISAX® a jeho implementácii.

Prínosy?

Implementácia softvéru pre riadenie štandardu TISAX® prináša nasledovné prínosy:
Zvýšenie informačnej bezpečnosti: Softvér umožňuje komplexnú implementáciu a udržiavanie požiadaviek TISAX®, čím sa znižuje riziko kybernetických útokov a ochranu citlivých informácií. Zjednodušenie auditov: Softvér uľahčuje interný a externý audit súladu s TISAX® a automatizuje reporting. Zníženie nákladov: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadu môže priniesť značné úspory nákladov. Zlepšenie reputácie: Preukázanie záväzku k informačnej bezpečnosti a súladu s TISAX® posilňuje dôveru partnerov a zákazníkov. Zvýšenie konkurencieschopnosti: Dodržiavanie štandardu TISAX® môže zlepšiť konkurencieschopnosť na trhu automobilového priemyslu.

NAKIB

SOFTWAROVÉ VYBAVENIE

Software pre riadenie biznis kontinuity

APLIKÁCIA NA PODPORU RIADENIE BCM V ROZSAHU VYKONANIA BIA PODĽA ISO 22317

Čo je?

Softvér na riadenie kontinuity biznisu (BCMS) je nástroj, ktorý pomáha organizáciám definovať, implementovať a udržiavať stratégie a procesy na zaistenie kontinuity prevádzky v prípade neočakávaných udalostí. Softvér môže mať rôzne funkcie, ako napríklad:
Identifikácia rizík: Pomáha pri identifikácii a hodnotení rizík, ktoré by mohli narušiť prevádzku organizácie. Plánovanie kontinuity: Umožňuje definovať plány kontinuity pre rôzne typy krízových scenárov. Implementácia a testovanie: Uľahčuje implementáciu a testovanie plánov kontinuity. Monitorovanie a reporting: Poskytuje nástroje na monitorovanie a reporting o stave kontinuity biznisu.

Prečo?

Zavedenie softvéru BCMS prináša viacero benefitov:
Zvýšená odolnosť: Zvýšenie odolnosti organizácie voči neočakávaným udalostiam a minimalizácia ich dopadu na prevádzku. Rýchle obnovenie prevádzky: Zrýchlenie obnovenia prevádzky v prípade krízy a minimalizácia prestojov. Zníženie strát: Zníženie finančných a reputačných strát súvisiacich s krízovými situáciami. Zlepšenie dodržiavania regulácií: Zabezpečenie súladu s regulačnými požiadavkami na riadenie kontinuity biznisu. Zvýšenie informovanosti: Zvýšenie informovanosti manažmentu a zamestnancov o rizikách a plánoch kontinuity.

Pre koho?

Softvér BCMS je určený pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za riadenie kontinuity biznisu v rámci svojej organizačnej jednotky. IT profesionálov: Ktorí sa podieľajú na implementácii a údržbe softvéru BCMS.
Audítorov: Ktorí sa venujú auditu riadenia kontinuity biznisu. Konzultantov: Ktorí poskytujú poradenstvo v oblasti riadenia kontinuity biznisu. Každý, kto sa chce dozvedieť viac o riadení kontinuity biznisu.

Prínosy?

Implementácia softvéru BCMS prináša nasledovné prínosy:
Zvýšená odolnosť voči krízovým situáciám: Softvér umožňuje komplexnú identifikáciu a hodnotenie rizík, definovanie a implementáciu plánov kontinuity a efektívne riadenie krízových situácií. Rýchle obnovenie prevádzky: Automatizácia procesov a centralizované uchovávanie informácií v softvéri umožňuje rýchle a efektívne obnovenie prevádzky po kríze. Zníženie strát: Predchádzanie krízovým situáciám a minimalizácia ich dopadu môže priniesť značné úspory nákladov a minimalizovať reputačné straty. Zlepšenie informovanosti a koordinácie: Softvér umožňuje efektívnu komunikáciu a koordináciu medzi rôznymi tímami v rámci krízovej situácie. Zvýšenie konkurencieschopnosti: Preukázanie záväzku k riadeniu kontinuity biznisu posilňuje dôveru partnerov a zákazníkov a môže zlepšiť konkurencieschopnosť na trhu.