NÁRODNÁ AKADÉMIA PRE KYBERNETICKÚ A INFORMAČNÚ BEZPEČNOSŤ

KATALÓG SLUŽIEB 2024

NAKIB.SK

NAKIB

PORADENSKÉ SLUŽBY

Implementácia Cyber Security podľa ZoKB 69/2018

Implementácia Cyber Security podľa NIS2

Implementácia ISO 9001

Implementácia ISO 27001

Implementácia ISO 27005

Implementácia ISO 20000

Implementácia IEC 62443

Implementácia Biznis kontinuity (BCM)

Implementácia požiadaviek GDPR

Implementácia požiadaviek TISAX®

Implementácia požiadaviek DORA

Poskytovanie Vulnerability Manažmentu

Vykonávanie PEN Testov

Napojenie na SIEM system

Zabezpečenie Cloudových služieb

NAKIB.SK

NAKIB

ŠKOLENIA

Manažér kyber bezpečnosti (MKB)

Audítor kyber bezpečnosti (AKB)

Manažér pre kyber bezpečnosť MKB podľa NIS2

TISAX® Manažér pre informačnú bezpečnosť v automotív

Nová norma ISO 27001:2022

Vykonávanie analýzy rizík

Manažér pre riadenie kontinuity činností

Znalosti Zákona o ITVS 95/2019

Požiadavky v oblasti ochrany osobných údajov v zmysle GDPR

Základy hackingu

DORA

Zákon o utajovaných skutočnostiach 215/2004 Z. z.

AI - Umelá inteligencia

Kybernetická bezpečnosť v OT prostredí

NAKIB.SK

NAKIB

AUDIT A GAP ANALÝZY

Cyber Security
zákon 69 ZoKB

Cyber Security NIS

Verejná správa ITVS

DORA, Finančný
sektor

ISO 27001

BCM

ISO 20000

IEC 62443

ISO 9001

GDPR

TISAX

Cloudové služby

Aplikačný audit
podľa ISVS OWASP

NAKIB.SK

NAKIB

E-LEARNINGOVÉ SLUŽBY

Základy informačnej bezpečnosti

Základy kyber bezpečnosti

Základy ochrany osobných údajov

Základy biznis kontinuity

Základy TISAX

TISAX Pokročilí

NAKIB

OUTSOURCOVANÉ ROLE

DORA

Výkon MKB

Výkon DPO

Výkon IA

Výkon SOC Služieb

NAKIB.SK

NAKIB

SOFTWAROVÉ VYBAVENIE

Software pre
Analýzu rizík ICT

Software pre
Analýzu rizík privacy

Software pre
Analýzu rizík,
Protikorupčný
systém

Software pre riadenie
štandardu TISAX

Riadenie Biznis
Kontinuity

NAKIB

ŠKOLENIA PRE SOC SLUŽBY

Real World
Penetration testing

Real World
forensics analysis

Real World
incident response

NAKIB.SK

NAKIB

PORADENSKÉ SLUŽBY

NAKIB.SK

PORADENSTVO A POSKYTOVANIE SLUŽIEB V OBLASTI KYBER BEZPEČNSTI PODĽA ZOKB A JEDNOTLIVÝCH VYHLÁŠOK

Čo je?

Zákon o kybernetickej bezpečnosti (ZoKB) č. 69/2018 Z. z. definuje právne a technické požiadavky na kybernetickú bezpečnosť prevádzkovateľov základných služieb a orgánov verejnej moci. Cieľom je chrániť informačné systémy a siete pred kybernetickými hrozbami a incidentmi.

Prečo?

Implementácia kybernetickej bezpečnosti podľa ZoKB prináša viacero benefitov:
Zvýšenie ochrany informačných systémov a sietí: Znižuje sa riziko kybernetických útokov a narušení, čím sa chránia citlivé údaje a kritická infraštruktúra.
Posilnenie dôveryhodnosti a reputácie: Prevádzkovatelia demonštrujú zodpovedný prístup k ochrane informácií a budovaniu odolnosti voči kybernetickým hrozbám.
Zníženie rizika finančných a reputačných strát: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadov šetrí finančné prostriedky a chráni reputáciu organizácie.
Spolnenie zákonných požiadaviek: Implementácia ZoKB je povinná pre prevádzkovateľov základných služieb a orgány verejnej moci.

Pre koho?

Zákon sa týka nasledovných subjektov:
Prevádzkovatelia základných služieb: Poskytovatelia kritických služieb v oblastiach ako energetika, doprava, financie, zdravotníctvo a digitálne služby.
Orgány verejnej moci: Štátne orgány, samosprávy a verejnoprávne inštitúcie.

Prínosy?

Implementácia kybernetickej bezpečnosti podľa ZoKB prináša nasledovné prínosy:
Zvýšená ochrana: Znižuje sa riziko krádeže dát, výpadkov služieb a narušenia prevádzky.
Posilnená odolnosť: Organizácia je lepšie pripravená na odrazenie a reakciu na kybernetické incidenty.
Zvýšená dôvera: Zákazníci a partneri vnímajú organizáciu ako zodpovednú a dôveryhodnú.
Zníženie nákladov: Predchádzanie incidentom a minimalizácia ich dopadov šetrí finančné prostriedky.

PORADENSTVO A POSKYTOVANIE SLUŽIEB V OBLASTI CYBER SECURITY NIS

Čo je?

Smernica o opatreniach na vysokú úroveň kybernetickej bezpečnosti v Únii (NIS2) je aktualizovaná legislatíva EÚ, ktorá nahradila pôvodnú smernicu NIS z roku 2016.

Prečo?

Implementácia kybernetickej bezpečnosti podľa NIS2 prináša viacero benefitov:
Zvýšená ochrana kľúčových sektorov: Posilňuje sa ochrana kritickej infraštruktúry a služieb v oblastiach ako energetika, doprava, financie, zdravotníctvo a digitálne služby.
Zvýšená odolnosť: Organizácie sú lepšie pripravené na odrazenie a reakciu na kybernetické incidenty.
Posilnená dôvera: Zákazníci a partneri vnímajú organizáciu ako zodpovednú a dôveryhodnú.
Zníženie rizika sankcií: Nesplnenie požiadaviek NIS2 môže viesť k sankciám zo strany regulačných orgánov.

Pre koho?

NIS2 sa týka nasledovných subjektov:
Prevádzkovatelia tzv. “**esenciálnych služieb**”: Poskytovatelia kritických služieb v oblastiach ako energetika, doprava, financie, zdravotníctvo a digitálne služby.
“**Dôležití poskytovatelia služieb**”: Poskytovatelia digitálnych služieb, ako sú online obchody, vyhľadávače a cloudové služby.

Prínosy?

Implementácia kybernetickej bezpečnosti podľa NIS2 prináša nasledovné prínosy:
Zvýšená ochrana: Znižuje sa riziko krádeže dát, výpadkov služieb a narušenia prevádzky.
Posilnená odolnosť: Organizácia je lepšie pripravená na odrazenie a reakciu na kybernetické incidenty.
Zvýšená dôvera: Zákazníci a partneri vnímajú organizáciu ako zodpovednú a dôveryhodnú.
Zníženie rizika sankcií: Splnenie požiadaviek NIS2 chráni pred sankciami zo strany regulačných orgánov.

PORADENSTVO ISMS (SYSTÉM RIADENIA KVALITY), PLATNOSŤ CERTIFIKÁCIE 3 ROKY, DOZORNÝ AUDIT ROČNE

Čo je?

ISO 9001 je medzinárodná norma pre systémy manažérstva kvality. Poskytuje súbor požiadaviek a osvedčených postupov, ktoré pomáhajú organizáciám efektívne riadiť a zlepšovať svoje procesy s cieľom dosiahnuť **trvalé uspokojenie zákazníkov**.

Prečo?

Implementácia ISO 9001 prináša viacero benefitov:
Zlepšenie kvality produktov a služieb: Systém manažérstva kvality pomáha organizácii identifikovať a eliminovať chyby v procesoch, čím sa zvyšuje kvalita produktov a služieb.
Zvýšenie spokojnosti zákazníkov: Zameranie na požiadavky a očakávania zákazníkov vedie k ich vyššej spokojnosti a lojalite. **Zvýšenie efektivity procesov:** Optimalizácia procesov a eliminácia plytvania vedie k zníženiu nákladov a zlepšeniu produktivity. **Posilnenie konkurencieschopnosti:** Implementácia ISO 9001 demonštruje záväzok organizácie k trvalému zlepšovaniu a posilňuje jej reputáciu na trhu. Zjednodušenie prístupu k tendrom: Mnoho verejných obstarávaní vyžaduje od uchádzačov certifikáciu ISO 9001.

Pre koho?

Norma ISO 9001 je univerzálna a môže sa **implementovať v akomkoľvek type organizácie**, bez ohľadu na jej veľkosť, oblasť pôsobnosti alebo stupeň zrelosti. Je vhodná pre:
Výrobné firmy: Zlepšuje riadenie výrobných procesov a kvalitu produktov.
Poskytovateľov služieb: Zlepšuje kvalitu služieb a zákaznícky servis.
Neziskovky: Zvyšuje efektivitu a transparentnosť fungovania organizácie.
Verejný sektor: Zlepšuje kvalitu verejných služieb a zodpovednosť voči občanom.

Prínosy?

Implementácia ISO 9001 prináša nasledovné prínosy:

Zvýšená dôvera: Zákazníci a partneri vnímajú organizáciu ako zodpovednú a spoľahlivú.
Lepšie riadenie rizík: Systém manažérstva kvality pomáha predchádzať chybám a eliminovať riziká.
Motivácia zamestnancov: Zapojenie zamestnancov do procesu zlepšovania posilňuje ich motiváciu a lojalitu.
Zlepšenie firemnej kultúry: Zameranie na kvalitu a neustále zlepšovanie vytvára pozitívnu firemnú kultúru.

PORADENSTVO V OBLASTI PRÍPRAVY NA CERTIFIKÁCIU ISMS (SYSTÉM RIADENIA INFORMAČNEJ BEZPEČNOSTI)

Čo je?

ISO/IEC 27001 je medzinárodná norma pre systémy manažérstva informačnej bezpečnosti. Poskytuje súbor požiadaviek a osvedčených postupov, ktoré pomáhajú organizáciám chrániť svoje informačné aktíva pred rôznymi hrozbami a incidentmi.

Prečo?

Implementácia ISO/IEC 27001 prináša viacero benefitov:
Zvýšenie informačnej bezpečnosti: Systém manažérstva informačnej bezpečnosti pomáha organizácii identifikovať a riadiť riziká týkajúce sa dôvernosti, integrity a dostupnosti informácií. Zníženie rizika kybernetických útokov: Implementácia kontrolných mechanizmov a osvedčených postupov znižuje riziko úspešných kybernetických útokov a narušenia informačných systémov. Posilnenie dôvery zákazníkov a partnerov: Certifikácia ISO/IEC 27001 demonštruje záväzok organizácie k ochrane informácií a posilňuje jej reputáciu na trhu. Zlepšenie súladu s regulačnými požiadavkami: Norma ISO/IEC 27001 integruje požiadavky rôznych regulačných predpisov na ochranu osobných údajov a informačnej bezpečnosti.
Zvýšenie efektivity riadenia informácií: Implementácia systému manažérstva informačnej bezpečnosti vedie k efektívnejšiemu riadeniu a ochrane informačných aktív.

Pre koho?

Norma ISO/IEC 27001 je univerzálna a môže sa implementovať v akomkoľvek type organizácie, bez ohľadu na jej veľkosť, oblasť pôsobnosti alebo stupeň zrelosti. Je vhodná pre:
Súkromné firmy: Zlepšuje ochranu citlivých informácií a obchodných tajomstiev.
Verejné inštitúcie: Zvyšuje bezpečnosť a dôveryhodnosť pri práci s citlivými údajmi občanov.
Neziskovky: Chráni informácie o darcoch, klientoch a interných procesoch.
Organizácie v regulovaných odvetviach: Uľahčuje splnenie požiadaviek na ochranu osobných údajov a informačnej bezpečnosti.

Prínosy?

Implementácia ISO/IEC 27001 prináša nasledovné prínosy:
Zníženie nákladov: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadov šetrí finančné prostriedky. Zvýšenie produktivity: Zníženie výpadkov a narušení prevádzky súvisiacich s informačnou bezpečnosťou. Posilnenie konkurencieschopnosti: Demonštrovanie záväzku k ochrane informácií a budovanie odolnosti voči kybernetickým hrozbám. Zlepšenie firemnej kultúry: Zvýšenie povedomia o informačnej bezpečnosti a zodpovednosti zamestnancov.

NAKIB

PORADENSKÉ SLUŽBY

Implementácia ISO 27005

PORADENSTVO V OBLASTI RIADENIA RIZÍK AKO MANDATORNEJ POVINNOSTI PRE ISO 9K1, ISO 27K1, GDPR

Čo je?

ISO/IEC 27005 je medzinárodná norma, ktorá poskytuje usmernenia pre riadenie rizík informačnej bezpečnosti v súlade s normou ISO/IEC 27001. Norma definuje procesy a postupy na identifikáciu, hodnotenie a riadenie rizík súvisiacich s informačnými aktívami organizácie.

Prečo?

Implementácia ISO/IEC 27005 prináša viacero benefitov:
Zlepšenie riadenia rizík: Norma poskytuje systematický prístup k identifikácii, analýze a riadeniu rizík informačnej bezpečnosti. Zvýšenie efektívnosti: Optimalizácia procesov riadenia rizík znižuje čas a náklady na riešenie bezpečnostných incidentov. Posilnenie súladu s normami: Implementácia ISO/IEC 27005 podporuje súlad s požiadavkami ISO/IEC 27001 a ostatných regulačných predpisov. Zvýšenie informovanosti manažmentu: Poskytuje manažmentu jasný prehľad o rizikách informačnej bezpečnosti a ich dopadoch na organizáciu. Zlepšenie firemnej kultúry: Podporuje zodpovedné správanie zamestnancov pri práci s informáciami.

Pre koho?

Norma ISO/IEC 27005 je určená pre organizácie, ktoré už implementovali systém manažérstva informačnej bezpečnosti podľa ISO/IEC 27001 a chcú posilniť riadenie rizík v tejto oblasti. Je vhodná pre:
Súkromné firmy: Zlepšuje riadenie rizík súvisiacich s ochranou citlivých informácií a obchodných tajomstiev.
Verejné inštitúcie: Zvyšuje efektivitu riadenia rizík pri práci s citlivými údajmi občanov.
Neziskovky: Posilňuje ochranu informácií o darcoch, klientoch a interných procesoch.
Organizácie v regulovaných odvetviach: Uľahčuje splnenie požiadaviek na ochranu osobných údajov a informačnej bezpečnosti.

Prínosy?

Implementácia ISO/IEC 27005 prináša nasledovné prínosy:
Zníženie rizika kybernetických útokov: Lepšie pochopenie a riadenie rizík znižuje pravdepodobnosť úspešných kybernetických útokov. Zníženie finančných strát: Predchádzanie incidentom a minimalizácia ich dopadov šetrí finančné prostriedky. Posilnenie reputácie: Demonštrovanie záväzku k proaktívnemu riadeniu rizík posilňuje dôveru zákazníkov a partnerov.Zvýšenie konkurencieschopnosti: Zlepšenie odolnosti voči kybernetickým hrozbám a ochrana kľúčových informácií.

PORADENSTVO V OBLASTI PRÍPRAVY NA CERTIFIKÁCIU (SYSTÉM RIADENIA ICT SLUŽIEB)

Čo je?

ISO 20000-1 je medzinárodná norma, ktorá definuje požiadavky na systém manažérstva služieb IT (SMS). Norma stanovuje súbor osvedčených postupov pre efektívne riadenie a dodávanie IT služieb v súlade s požiadavkami zákazníkov a s ohľadom na neustále zlepšovanie.

Prečo?

Implementácia ISO 20000-1 prináša viacero benefitov:
Zvýšenie kvality IT služieb: Norma podporuje systematický prístup k riadeniu IT služieb, čím sa zvyšuje ich kvalita a spoľahlivosť. Zlepšenie spokojnosti zákazníkov: Zameranie na požiadavky a očakávania zákazníkov vedie k ich vyššej spokojnosti a lojalite. Zvýšenie efektivity procesov: Optimalizácia procesov a eliminácia plytvania vedie k zníženiu nákladov a zlepšeniu produktivity. Posilnenie konkurencieschopnosti: Implementácia ISO 20000-1 demonštruje záväzok organizácie k trvalému zlepšovaniu a posilňuje jej reputáciu na trhu. Zjednodušenie prístupu k tendrom: Mnoho verejných obstarávaní v oblasti IT vyžaduje od uchádzačov certifikáciu ISO 20000-1.

Pre koho?

Norma ISO 20000-1 je univerzálna a môže sa implementovať v akomkoľvek type organizácie, ktorá poskytuje IT služby, bez ohľadu na jej veľkosť, oblasť pôsobnosti alebo stupeň zrelosti.
Je vhodná pre:
Poskytovateľov IT služieb: Zlepšuje riadenie a dodávanie IT služieb rôznym typom klientov.
Interné IT oddelenia: Zvyšuje efektivitu a kvalitu interných IT služieb v rámci organizácie.
Vývojárske firmy: Zlepšuje procesy vývoja a dodávania softvéru.
Organizácie s rozsiahlymi IT systémami: Posilňuje riadenie a kontrolu nad komplexnou IT infraštruktúrou.

Prínosy?

Implementácia ISO 20000-1 prináša nasledovné prínosy:
Zvýšenie dôvery: Zákazníci a partneri vnímajú organizáciu ako zodpovednú a spoľahlivú.
Lepšie riadenie rizík: Systém manažérstva služieb IT pomáha predchádzať incidentom a eliminovať riziká súvisiace s IT službami. Motivácia zamestnancov: Zapojenie zamestnancov do procesu zlepšovania posilňuje ich motiváciu a lojalitu. Zlepšenie firemnej kultúry: Zameranie na kvalitu a neustále zlepšovanie vytvára pozitívnu firemnú kultúru v oblasti IT.

PORADENSTVO V OBLASTI PRÍPRAVY NA CERTIFIKÁCIU (PRIEMYSELNA BEZPEČNOSŤ)

Čo je?

IEC 62443 je séria medzinárodných noriem, ktorá definuje požiadavky na kybernetickú a informačnú bezpečnosť priemyselných automatizačných a riadiacich systémov (IACS). Tieto normy stanovujú súbor osvedčených postupov pre ochranu IACS pred rôznymi hrozbami a incidentmi.

Prečo?

Implementácia IEC 62443 prináša viacero benefitov:
Zvýšenie kybernetickej bezpečnosti IACS: Normy definujú komplexné bezpečnostné opatrenia na ochranu IACS pred kybernetickými útokmi a narušeniami.
Zníženie rizika výpadkov a porúch: Zvýšená odolnosť IACS znižuje riziko výpadkov prevádzky a porúch, ktoré by mohli viesť k značným finančným stratám.
Posilnenie súladu s regulačnými požiadavkami: IEC 62443 integruje požiadavky rôznych regulačných predpisov na kybernetickú bezpečnosť v priemyselnom sektore.
Zlepšenie ochrany kritickej infraštruktúry: Implementácia noriem posilňuje ochranu kritickej infraštruktúry, ako sú elektrárne, vodárenské systémy a dopravné systémy.
Zvýšenie dôvery a reputácie: Demonštrovanie záväzku k kybernetickej bezpečnosti posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu.

Pre koho?

Norma IEC 62443 je určená pre prevádzkovateľov a vlastníkov IACS v rôznych priemyselných odvetviach, ako sú: Energetika: Elektrárne, distribučné siete, prenosové sústavy.
Doprava: Letecká doprava, železničná doprava, cestná doprava, vodná doprava.
Vodárenstvo: Vodárenské systémy, čističky odpadových vôd.
Výroba: Automobilový priemysel, chemický priemysel, farmaceutický priemysel.
Kritická infraštruktúra: Ropovodné a plynové systémy, telekomunikácie, systémy riadenia budov.

Prínosy?

Implementácia IEC 62443 prináša nasledovné prínosy:
Zníženie nákladov: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadov šetrí finančné prostriedky.
Zvýšenie produktivity: Zníženie výpadkov a narušení prevádzky súvisiacich s kybernetickou bezpečnosťou.
Posilnenie konkurencieschopnosti: Demonštrovanie záväzku k ochrane IACS a budovanie odolnosti voči kybernetickým hrozbám.
Zlepšenie firemnej kultúry: Zvýšenie povedomia o kybernetickej bezpečnosti a zodpovednosti zamestnancov.

PORADENSTVO V OBLASTI PRÍPRAVY NA CERTIFIKÁCIU BIZNIS KONTINUITA PODĽA ISO 22301

Čo je?

BCM, skrátene pre Business Continuity Management, je strategický rámec pre riadenie kontinuity podnikania. Zahŕňa súbor procesov a aktivít, ktoré zaisťujú schopnosť poskytovania služieb aj počas krízy.

Prečo?

Implementácia BCM prináša viacero benefitov:
Zvýšenie odolnosti voči krízovým situáciám: BCM umožňuje organizácii rýchlo a efektívne reagovať na neočakávané udalosti a minimalizovať ich dopad na prevádzku. Zníženie rizika strát: Rýchle obnovenie kritických funkcií znižuje finančné straty a reputáciu, ktoré by mohli vzniknúť v dôsledku výpadku. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k kontinuite podnikania posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu. Zlepšenie firemnej kultúry: Zvýšenie povedomia o dôležitosti kontinuity podnikania a zodpovednosti zamestnancov. Spĺňanie regulačných požiadaviek: V niektorých odvetviach je implementácia BCM legislatívne podmienená.

Pre koho?

BCM je relevantný pre všetky typy organizácií, bez ohľadu na ich veľkosť, oblasť pôsobnosti alebo stupeň zrelosti. Je obzvlášť dôležitý pre:
Organizácie s kritickou infraštruktúrou: Poskytovatelia energií, telekomunikácií, dopravy a ďalších kritických služieb musia mať zaistenú kontinuitu prevádzky aj v krízových situáciách. Finančné inštitúcie: Banky, poisťovne a iné finančné inštitúcie musia chrániť svoje dáta a systémy pred narušením a výpadkami.
Veľké a komplexné organizácie: Rozsiahle firmy s rozsiahlymi sieťami a systémami potrebujú robustný systém riadenia kontinuity podnikania. Organizácie v regulovaných odvetviach: V niektorých odvetviach je implementácia BCM legislatívne podmienená.

Prínosy?

Implementácia BCM prináša nasledovné prínosy:
Zníženie nákladov: Predchádzanie stratám a minimalizácia dopadov krízových udalostí šetrí finančné prostriedky. Zvýšenie produktivity: Rýchle obnovenie prevádzky po krízových udalostiach minimalizuje straty produktivity. Posilnenie konkurencieschopnosti: Demonštrovanie odolnosti voči krízovým situáciám posilňuje konkurenčnú pozíciu organizácie. Zlepšenie morálky zamestnancov: Vedomie, že organizácia je pripravená na krízové situácie, zvyšuje morálku a motiváciu zamestnancov.

NAKIB

PORADENSKÉ SLUŽBY

Implementácia požiadaviek GDPR

PORADENSTVO V OBLASTI PRÍPRAVY NA ZABEZPEČENIE SÚLADU S NARIADENÍM GDPR

Čo je?

GDPR je skratka pre General Data Protection Regulation, v slovenčine nazývané aj Všeobecné nariadenie o ochrane údajov. Jedná sa o nariadenie Európskej únie, ktoré stanovuje pravidlá pre spracovanie osobných údajov fyzických osôb na území EÚ. Cieľom GDPR je chrániť súkromie a základné práva a slobody fyzických osôb a zároveň uľahčiť voľný pohyb osobných údajov v rámci EÚ.

Prečo?

Implementácia GDPR prináša viacero benefitov:
Zvýšenie ochrany osobných údajov: GDPR stanovuje prísne požiadavky na spracovanie osobných údajov, čím sa zvyšuje ich ochrana pred zneužitím. Zníženie rizika pokút: Porušenie GDPR môže viesť k vysokým pokutám, preto je dôležité mať implementované adekvátne bezpečnostné opatrenia. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k ochrane osobných údajov posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu. Zlepšenie firemnej kultúry: Zvýšenie povedomia o dôležitosti ochrany osobných údajov a zodpovednosti zamestnancov. Spĺňanie regulačných požiadaviek: GDPR je záväzné pre všetky organizácie, ktoré spracúvajú osobné údaje fyzických osôb v EÚ.

Pre koho?

GDPR sa vzťahuje na všetky organizácie, ktoré spracúvajú osobné údaje fyzických osôb v EÚ, bez ohľadu na ich veľkosť, oblasť pôsobnosti alebo sídlo. To zahŕňa:
Súkromné firmy: Všetky firmy, ktoré spracúvajú osobné údaje svojich zákazníkov, zamestnancov, dodávateľov a ďalších osôb. Verejné inštitúcie: Štátne orgány, úrady a verejné inštitúcie, ktoré spracúvajú osobné údaje v rámci svojej činnosti. Neziskovky: Neziskové organizácie a združenia, ktoré spracúvajú osobné údaje svojich členov, darcov a dobrovoľníkov. Fyzické osoby: Aj fyzické osoby, ktoré spracúvajú osobné údaje v rámci svojej profesie alebo inej činnosti.

Prínosy?

Implementácia GDPR prináša nasledovné prínosy:
Zníženie nákladov: Predchádzanie sankciám za porušenie GDPR a minimalizácia dopadov incidentov súvisiacich s ochranou osobných údajov šetrí finančné prostriedky. Zvýšenie produktivity: Zvýšenie efektivity spracovania osobných údajov a zníženie administratívnej záťaže. Posilnenie konkurencieschopnosti: Demonštrovanie zodpovedného prístupu k ochrane osobných údajov posilňuje konkurenčnú pozíciu organizácie na trhu. Zlepšenie imidžu a reputácie: Posilnenie dôvery verejnosti v organizáciu a jej záväzok k etickému spracovaniu osobných údajov.

PORADENSTVO V OBLASTI PRÍPRAVY NA AUDIT TISAX®

Čo je?

TISAX je skratka pre Trusted Information Security Assessment Exchange. Jedná sa o mechanizmus hodnotenia a výmeny informácií o informačnej bezpečnosti v automobilovom priemysle.

Prečo?

Implementácia TISAX prináša viacero benefitov:
Zvýšenie kybernetickej bezpečnosti: TISAX stanovuje prísne požiadavky na riadenie informačnej bezpečnosti, čím sa znižuje riziko kybernetických útokov a narušení. Zlepšenie dodávateľského reťazca: TISAX umožňuje automobilovým výrobcom a dodávateľom zdieľať informácie o kybernetickej bezpečnosti a budovať dôveru v rámci dodávateľského reťazca. Zníženie nákladov: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadov šetrí finančné prostriedky. Posilnenie konkurencieschopnosti: Demonštrovanie záväzku k informačnej bezpečnosti posilňuje konkurenčnú pozíciu na trhu automobilového priemyslu.
Spĺňanie požiadaviek odberateľov: Mnoho automobilových výrobcov a dodávateľov vyžaduje od svojich partnerov certifikáciu TISAX.

Pre koho?

TISAX je určený pre všetky organizácie v automobilovom priemysle, ktoré spracúvajú citlivé informácie, ako napríklad:

Výrobcovia automobilov: OEM (Original Equipment Manufacturer) a Tier 1 dodávatelia.
Dodávatelia komponentov: Tier 2 a Tier 3 dodávatelia.
Poskytovatelia služieb: Poskytovatelia IT služieb, logistické firmy a iné subjekty v dodávateľskom reťazci.

Prínosy?

Implementácia TISAX prináša nasledovné prínosy:

Zvýšenie dôvery: Zákazníci a partneri vnímajú organizáciu ako zodpovednú a spoľahlivú v oblasti informačnej bezpečnosti.
Lepšie riadenie rizík: Systém manažérstva informačnej bezpečnosti TISAX pomáha predchádzať kybernetickým incidentom a eliminovať riziká súvisiace s informačnou bezpečnosťou.
Motivácia zamestnancov: Zapojenie zamestnancov do procesu zlepšovania informačnej bezpečnosti posilňuje ich motiváciu a lojalitu.
Zlepšenie firemnej kultúry: Zameranie na kybernetickú bezpečnosť a ochranu citlivých informácií vytvára pozitívnu firemnú kultúru.

PORADENSTVO V OBLASTI PRÍPRAVY NA MEDZINÁRODNÉHO ŠTANDARDU DORA PRE FINANČNÉ SLUŽBY

Čo je?

DORA je skratka pre Digital Operational Resilience Act, v slovenčine nazývané aj Akt o digitálnej prevádzkovej odolnosti. Jedná sa o nariadenie Európskej únie, ktoré stanovuje požiadavky na riadenie digitálnej prevádzkovej odolnosti (DORA) v sektore finančných služieb. Cieľom DORA je posilniť odolnosť finančného sektora voči digitálnym hrozbám a incidentom.

Prečo?

Implementácia DORA prináša viacero benefitov:
Zvýšenie odolnosti voči kybernetickým hrozbám: DORA stanovuje prísne požiadavky na riadenie digitálnych rizík, čím sa znižuje riziko kybernetických útokov a narušení prevádzky. Zníženie finančných strát: Predchádzanie incidentom a minimalizácia ich dopadov šetrí finančné prostriedky a chráni reputáciu finančných inštitúcií.Posilnenie dôvery a stability: Demonštrovanie záväzku k digitálnej odolnosti posilňuje dôveru zákazníkov a investorov v stabilitu finančného sektora.Zlepšenie súladu s regulačnými požiadavkami: DORA integruje požiadavky rôznych regulačných predpisov na kybernetickú a informačnú bezpečnosť v sektore finančných služieb.Zvýšenie konkurencieschopnosti: Implementácia DORA môže posilniť konkurenčnú pozíciu finančných inštitúcií, ktoré demonštrujú proaktívny prístup k riadeniu digitálnych rizík.

Pre koho?

DORA sa vzťahuje na všetky subjekty pôsobiace v sektore finančných služieb v EÚ, ako napríklad:
Banky: Všetky typy bánk, vrátane retailových bánk, investičných bánk a centrálnych bánk.
Poisťovne: Všetky typy poisťovní, vrátane životných poisťovní, neživotných poisťovní a zaisťovní.
Investičné firmy: Investičné fondy, správcovské spoločnosti, makléri a iné subjekty poskytujúce investičné služby. Platobné inštitúcie: Poskytovatelia platobných služieb, ako sú napríklad bankomaty, online platobné systémy a mobilné platby. Trhové infraštruktúry: Burzy cenných papierov, clearingové domy a depozitáre cenných papierov.

Prínosy?

Implementácia DORA prináša nasledovné prínosy:
Zníženie rizika výpadkov a porúch: Zvýšená odolnosť IT systémov a infraštruktúry znižuje riziko výpadkov prevádzky a porúch, ktoré by mohli viesť k značným finančným stratám. Lepšie riadenie incidentov: DORA definuje procesy a postupy pre efektívne riadenie kybernetických incidentov a minimalizáciu ich dopadov. Zvýšenie povedomia o kybernetickej bezpečnosti: Implementácia DORA zvyšuje povedomie o kybernetických hrozbách a dôležitosti ochrany citlivých informácií. Zlepšenie firemnej kultúry: Posilňuje zodpovednosť vedenia a zamestnancov za kybernetickú a informačnú bezpečnosť.

POSKYTOVANIE SLUŽIEB VULNERABILITY MANAGEMENTU ALEBO ZAVEDENIE PROCESU VULNERABILITY MANAŽMENT

Čo je?

Riadenie zraniteľností je systematický proces identifikácie, hodnotenia a riešenia zraniteľností v IT systémoch a softvéri. Cieľom riadenia zraniteľností je minimalizovať riziká kybernetických útokov a narušení prevádzky, ktoré by mohli viesť k finančným stratám, krádeži dát a strate reputácie.

Prečo?

Implementácia riadenia zraniteľností prináša viacero benefitov:
Zvýšenie kybernetickej bezpečnosti: Riadenie zraniteľností znižuje riziko úspešných kybernetických útokov a narušení prevádzky. Zníženie finančných strát: Predchádzanie incidentom a minimalizácia ich dopadov šetrí finančné prostriedky. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k kybernetickej bezpečnosti posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu.
Zlepšenie súladu s regulačnými požiadavkami: Mnoho regulačných predpisov vyžaduje od organizácií implementáciu riadenia zraniteľností. Zvýšenie produktivity: Zníženie výpadkov a porúch súvisiacich s kybernetickými útokmi.

Pre koho?

Riadenie zraniteľností je relevantné pre všetky typy organizácií, bez ohľadu na ich veľkosť, oblasť pôsobnosti alebo stupeň zrelosti. Je obzvlášť dôležité pre: Organizácie s kritickou infraštruktúrou: Poskytovatelia energií, telekomunikácií, dopravy a ďalších kritických služieb musia mať zaistenú ochranu svojich IT systémov pred zraniteľnosťami. Finančné inštitúcie: Banky, poisťovne a iné finančné inštitúcie musia chrániť svoje systémy a dáta pred kybernetickými útokmi. Veľké a komplexné organizácie: Rozsiahle firmy s rozsiahlymi sieťami a systémami potrebujú robustný systém riadenia zraniteľností. Organizácie v regulovaných odvetviach: V niektorých odvetviach je implementácia riadenia zraniteľností legislatívne podmienená.

Prínosy?

Implementácia riadenia zraniteľností prináša nasledovné prínosy:
Zníženie rizika kybernetických útokov: Včasná identifikácia a riešenie zraniteľností znižuje útočnú plochu pre hackerov. Rýchlejšia reakcia na incidenty: Schopnosť rýchlo identifikovať a reagovať na kybernetické incidenty minimalizuje ich dopady. Zlepšenie firemnej kultúry: Zvýšenie povedomia o kybernetických hrozbách a dôležitosti ochrany IT systémov. Lepšie riadenie IT rizík: Riadenie zraniteľností je dôležitou súčasťou celkového riadenia IT rizík v organizácii.

POSKYTOVANIE SLUŽIEB PENETRAČNÉHO TESTOVANIA

Čo je?

Penetráčné testy, skrátene PEN testy, sú simulované kybernetické útoky, ktoré sa vykonávajú s cieľom identifikovať a otestovať zraniteľnosti v IT systémoch a sieťach. Tieto testy sa realizujú z pohľadu útočníka.

Prečo?

Implementácia penetračných testov prináša viacero benefitov:
Zvýšenie kybernetickej bezpečnosti: Penetráčné testy odhaľujú skryté zraniteľnosti v IT systémoch, ktoré by mohli byť zneužité hackermi. Zníženie rizika kybernetických útokov: Včasná identifikácia a riešenie zraniteľností znižuje útočnú plochu pre hackerov. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k kybernetickej bezpečnosti posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu. Zlepšenie súladu s regulačnými požiadavkami: Mnoho regulačných predpisov vyžaduje od organizácií implementáciu penetračných testov. Zvýšenie efektivity IT infraštruktúry: Odhalenie a optimalizácia neefektívnych procesov v IT infraštruktúre.

Pre koho?

Penetráčné testy sú relevantné pre všetky typy organizácií, bez ohľadu na ich veľkosť, oblasť pôsobnosti alebo stupeň zrelosti. Je obzvlášť dôležité pre:
Organizácie s kritickou infraštruktúrou: Poskytovatelia energií, telekomunikácií, dopravy a ďalších kritických služieb musia mať zaistenú ochranu svojich IT systémov pred zraniteľnosťami.
Finančné inštitúcie: Banky, poisťovne a iné finančné inštitúcie musia chrániť svoje systémy a dáta pred kybernetickými útokmi. Veľké a komplexné organizácie: Rozsiahle firmy s rozsiahlymi sieťami a systémami potrebujú robustný systém riadenia kybernetickej bezpečnosti.
Organizácie v regulovaných odvetviach: V niektorých odvetviach je implementácia penetračných testov legislatívne podmienená.

Prínosy?

Implementácia penetračných testov prináša nasledovné prínosy:
Zníženie rizika finančných strát: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadov šetrí finančné prostriedky. Zvýšenie produktivity: Zníženie výpadkov a porúch súvisiacich s kybernetickými útokmi. Posilnenie konkurencieschopnosti: Demonštrovanie proaktívneho prístupu k kybernetickej bezpečnosti posilňuje konkurenčnú pozíciu na trhu. Zlepšenie firemnej kultúry: Zvýšenie povedomia o kybernetických hrozbách a dôležitosti ochrany IT systémov.

PORADENSTVO A POSKYTOVANIE SLUŽIEB PRI VÝBERE A IMPLEMENTÁCII SIEM SYSTÉMOV

Čo je?

SIEM systém je softvérová platforma, ktorá integruje a analyzuje bezpečnostné informácie a udalosti z rôznych zdrojov v rámci IT infraštruktúry organizácie. SIEM systém umožňuje centralizované monitorovanie a riadenie bezpečnostných incidentov, čím zefektívňuje a urýchľuje reakciu na hrozby.

Prečo?

Implementácia SIEM systému prináša viacero benefitov:
Zvýšenie kybernetickej bezpečnosti: SIEM systém umožňuje včasnú detekciu a reakciu na kybernetické hrozby a incidenty. Zníženie rizika kybernetických útokov: Proaktívna identifikácia a analýza bezpečnostných udalostí znižuje útočnú plochu pre hackerov. Posilnenie súladu s regulačnými požiadavkami: Mnoho regulačných predpisov vyžaduje od organizácií implementáciu SIEM systému. Zníženie nákladov: Centralizovaná správa bezpečnostných informácií a udalostí znižuje náklady na riadenie kybernetickej bezpečnosti. Zlepšenie firemnej kultúry: Zvýšenie povedomia o kybernetických hrozbách a dôležitosti ochrany IT systémov.

Pre koho?

SIEM systém je relevantný pre všetky typy organizácií, bez ohľadu na ich veľkosť, oblasť pôsobnosti alebo stupeň zrelosti. Je obzvlášť dôležitý pre:
Organizácie s kritickou infraštruktúrou: Poskytovatelia energií, telekomunikácií, dopravy a ďalších kritických služieb musia mať zaistenú ochranu svojich IT systémov pred kybernetickými hrozbami.
Finančné inštitúcie: Banky, poisťovne a iné finančné inštitúcie musia chrániť svoje systémy a dáta pred kyberneticky mi útokmi.Veľké a komplexné organizácie: Rozsiahle firmy s rozsiahlymi sieťami a systémami potrebujú robustný systém riadenia kybernetickej bezpečnosti. Organizácie v regulovaných odvetviach: V niektorých odvetviach je implementácia SIEM systému legislatívne podmienená.

Prínosy?

Implementácia SIEM systému prináša nasledovné prínosy:
Zvýšenie rýchlosti a efektivity reakcie na incidenty: Centralizovaná analýza a korelácia udalostí umožňuje rýchlejšiu identifikáciu a reakciu na kybernetické incidenty. Zníženie objemu falošných poplachov: Inteligentná analýza udalostí znižuje počet falošných poplachov a umožňuje zamerať sa na relevantné hrozby. Zlepšenie forenznej analýzy: SIEM systém umožňuje zhromažďovať a analyzovať komplexné informácie o kybernetických incidentoch, čo uľahčuje forenznú analýzu a identifikáciu páchateľov.

PORADENSTVO V OBLASTI CLOUDOVÝCH SLUŽIEB A ICH ZABEZPEČENIA

Čo je?

Cloudové služby sú model dodávania IT služieb, ako napríklad úložisko dát, výpočtový výkon, softvér a databázy, cez internet. Tieto služby sú dostupné na požiadanie a škálovateľné podľa potreby, čím sa eliminuje potreba investovať do vlastnej IT infraštruktúry.

Prečo?

Zníženie nákladov: Cloudové služby eliminujú potrebu investovať do vlastného hardvéru a softvéru, znižujú náklady na údržbu a správu IT infraštruktúry. Zvýšenie flexibility a škálovatelnosti: Cloudové služby sa dajú rýchlo a jednoducho škálovať podľa aktuálnych potrieb, čím sa eliminuje potreba predimenzovávať vlastnú infraštruktúru. Zvýšená dostupnosť a spoľahlivosť: Cloudové služby sú dostupné 24/7 a poskytujú vysokú úroveň redundancie a ochrany dát. Zjednodušenie správy IT: Cloudové služby zjednodušujú správu IT infraštruktúry a umožňujú zamerať sa na strategické úlohy. Prístup k najnovším technológiám: Cloudové služby umožňujú prístup k najnovším IT technológiám bez potreby investovať do ich obstarania a údržby.

Pre koho?

Cloudové služby sú relevantné pre všetky typy organizácií, bez ohľadu na ich veľkosť, oblasť pôsobnosti alebo stupeň zrelosti. Sú vhodné pre:
Malé a stredné firmy: Cloudové služby umožňujú malým a stredným firmám prístup k moderným IT riešeniam bez potreby investovať do vlastnej infraštruktúry. Veľké firmy: Veľké firmy s rozsiahlymi IT požiadavkami dokážu využiť cloudové služby na zníženie nákladov a zjednodušenie správy IT.
Startupy a rýchlo rastúce firmy: Cloudové služby umožňujú startupom a rýchlo rastúcim firmám rýchlo a jednoducho škálovať svoju IT infraštruktúru podľa potreby.
Neziskovky a verejná správa: Cloudové služby sú vhodné pre Neziskovky a verejnú správu z dôvodu nízkych vstupných nákladov a vysokej škálovateľnosti.

Prínosy?

Implementácia cloudových služieb prináša nasledovné prínosy:
Zvýšenie produktivity: Zamestnanci sa možu sústrediť na svoje core úlohy a nemusia sa starať o správu IT infraštruktúry.
Zlepšenie spolupráce: Cloudové služby uľahčujú spoluprácu medzi zamestnancami a tímami, aj keď sa nachádzajú na rôznych miestach.
Zvýšená mobilita: Cloudové služby umožňujú prístup k firemným dátam a aplikáciám odkiaľkoľvek a z akéhokoľvek zariadenia.
Zvýšená bezpečnosť: Cloudové služby ponúkajú vysokú úroveň bezpečnosti a ochrany dát.

NAKIB

ŠKOLENIA

NAKIB.SK

PRÍPRAVA NA CERTIFIKAČNÚ SKÚŠKU A VÝKON ROLE MANAŽÉRA KYBERNETICKEJ BEZPEČNOSTI, PODĽA POŽIADAVIEK UVEDENÝCH VO VYHLÁŠKE ZOKB Č. 492_2022

Čo je?

Školenie Manažér kybernetickej bezpečnosti je komplexný program, ktorý rozvíja znalosti a zručnosti potrebné na efektívne riadenie kybernetickej bezpečnosti v organizácii. Školenie sa zameriava na rôzne aspekty kybernetickej bezpečnosti, ako napríklad: Riadenie rizík: Identifikácia, analýza a hodnotenie rizík kybernetických útokov. Ochrana dát: Implementácia a dodržiavanie bezpečnostných opatrení na ochranu dát. Reagovanie na incidenty: Vytvorenie a implementácia plánu reakcie na kybernetické incidenty. Dodržiavanie predpisov: Pochopenie a dodržiavanie relevantných legislatívnych požiadaviek v oblasti kybernetickej bezpečnosti. Leadership: Vedenie tímu kybernetickej bezpečnosti a budovanie povedomia o kybernetickej bezpečnosti v celej organizácii.

Prečo?

Absolvovanie školenia Manažér kybernetickej bezpečnosti prináša viacero benefitov:
Zvýšenie kybernetickej bezpečnosti: Získanie znalostí a zručností potrebných na efektívne riadenie kybernetickej bezpečnosti a zníženie rizika kybernetických útokov. Zníženie finančných strát: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadov šetrí finančné prostriedky. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k kybernetickej bezpečnosti posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu. Zlepšenie súladu s regulačnými požiadavkami: Mnoho regulačných predpisov vyžaduje od organizácií implementáciu a dodržiavanie bezpečnostných opatrení.
Zvýšenie produktivity: Zníženie výpadkov a porúch súvisiacich s kybernetickými útokmi.

Pre koho?

Školenie Manažér kybernetickej bezpečnosti je určené pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za riadenie kybernetickej bezpečnosti v organizácii. IT profesionálov: Ktorí sa chcú špecializovať na oblasť kybernetickej bezpečnosti. Osoby zodpovedné za ochranu dát: V rámci organizácie. Audítorov informačných systémov: Ktorí sa chcú zamerať na audity kybernetickej bezpečnosti. Každý, kto sa chce dozvedieť viac o riadení kybernetickej bezpečnosti.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o kybernetickej bezpečnosti: Školenie pokrýva širokú škálu tém relevantných pre riadenie kybernetickej bezpečnosti. Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty riadenia kybernetickej bezpečnosti a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi. Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti a zručnosti v oblasti kybernetickej bezpečnosti. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti kybernetickej bezpečnosti.

NAKIB

ŠKOLENIA

Audítor kyber bezpečnosti (AKB)

PRÍPRAVA NA CERTIFIKAČNÚ SKÚŠKU A VÝKON ROLE AUDÍTOR KYBERNETICKEJ BEZPEČNOSTI, PODĽA POŽIADAVIEK UVEDENÝCH VO VYHLÁŠKE ZOKB Č. 492_2022

Čo je?

Školenie Audítor kybernetickej bezpečnosti je komplexný program, ktorý rozvíja znalosti a zručnosti potrebné na vykonávanie auditov kybernetickej bezpečnosti v organizáciách. Školenie sa zameriava na rôzne aspekty auditu kybernetickej bezpečnosti, ako napríklad: Metodika auditu: Získanie znalostí o rôznych typoch auditov a osvedčených postupoch v tejto oblasti. Hodnotenie rizík: Identifikácia, analýza a hodnotenie rizík kybernetických útokov v rámci auditu. Technické aspekty: Pochopenie bežných zraniteľností a technických kontrolných mechanizmov. Právne a regulačné požiadavky: Znalosť relevantných legislatívnych požiadaviek v oblasti kybernetickej bezpečnosti. Komunikačné a prezentačné zručnosti: Efektivita komunikácie s manažmentom a ostatnými zainteresovanými stranami o výsledkoch auditu.

Prečo?

Absolvovanie školenia Audítor kybernetickej bezpečnosti prináša viacero benefitov:
Zvýšenie kybernetickej bezpečnosti: Získanie znalostí a zručností potrebných na identifikáciu a riešenie slabín v kybernetickej bezpečnosti organizácie. Zníženie rizika kybernetických útokov: Včasná identifikácia a náprava zraniteľností znižuje riziko úspešných kybernetických útokov. Zlepšenie súladu s regulačnými požiadavkami: Audity kybernetickej bezpečnosti pomáhajú organizáciám splniť regulačné požiadavky v tejto oblasti. Zvýšenie dôvery a reputácie: Demonštrovanie záväzku k kybernetickej bezpečnosti posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu. Zlepšenie riadenia kybernetickej bezpečnosti: Audity kybernetickej bezpečnosti pomáhajú organizáciám identifikovať oblasti, v ktorých je potrebné zlepšiť riadenie kybernetickej bezpečnosti.

Pre koho?

Školenie Audítor kybernetickej bezpečnosti je určené pre:
IT profesionálov: Ktorí sa chcú špecializovať na oblasť auditovania kybernetickej bezpečnosti.
Audítorov informačných systémov: Ktorí sa chcú zamerať na audity kybernetickej bezpečnosti.
Zamestnancov v oblasti kybernetickej bezpečnosti: Ktorí chcú rozšíriť svoje znalosti a zručnosti v oblasti auditovania. Manažérov a vedúcich pracovníkov: Zodpovedných za riadenie kybernetickej bezpečnosti v organizácii. Každý, kto sa chce dozvedieť viac o auditovaní kybernetickej bezpečnosti.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o auditovaní kybernetickej bezpečnosti: Školenie pokrýva širokú škálu tém relevantných pre auditovanie kybernetickej bezpečnosti. Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty auditovania kybernetickej bezpečnosti a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi. Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti a zručnosti v oblasti auditovania kybernetickej bezpečnosti. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti kybernetickej bezpečnosti.

NAKIB

ŠKOLENIA

Manažér pre kyber bezpečnosť podľa NIS2 (MKB)

VÝROBNÉ SPOLOČNOSTI VRÁTANE PRODUCENTOV POTRAVÍN BUDÚ MUSIEŤ ZAVIESŤ SYSTÉMY INFORMAČNEJ A KYBERNETICKEJ BEZPEČNOSTI

Čo je?

Školenie Manažér pre kybernetickú bezpečnosť MKB podľa NIS2 je komplexný program, ktorý rozvíja znalosti a zručnosti potrebné na efektívne riadenie kybernetickej bezpečnosti v organizáciách v súlade s smernicou NIS2 (Smernica o opatreniach pre vysokú úroveň kybernetickej bezpečnosti). Školenie sa zameriava na rôzne aspekty kybernetickej bezpečnosti s dôrazom na požiadavky NIS2, ako napríklad: Riadenie rizík: Identifikácia, analýza a hodnotenie rizík kybernetických útokov v kontexte NIS2. Ochrana dát: Implementácia a dodržiavanie bezpečnostných opatrení na ochranu dát v súlade s NIS2. Reagovanie na incidenty: Vytvorenie a implementácia plánu reakcie na kybernetické incidenty v súlade s NIS2. Dodržiavanie predpisov: Pochopenie a dodržiavanie požiadaviek NIS2 a relevantných legislatívnych predpisov v oblasti kybernetickej bezpečnosti. Leadership: Vedenie tímu kybernetickej bezpečnosti a budovanie povedomia o kybernetickej bezpečnosti v celej organizácii s ohľadom na NIS2.

Prečo?

Absolvovanie školenia Manažér pre kybernetickú bezpečnosť MKB podľa NIS2 prináša viacero benefitov:
Zvýšenie kybernetickej bezpečnosti: Získanie znalostí a zručností potrebných na efektívne riadenie kybernetickej bezpečnosti a zníženie rizika kybernetických útokov v súlade s NIS2. Zníženie finančných strát: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadov šetrí finančné prostriedky. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k kybernetickej bezpečnosti a k dodržiavaniu požiadaviek NIS2 posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu. Zlepšenie súladu s regulačnými požiadavkami: Školenie sa zameriava na splnenie požiadaviek NIS2 a relevantných legislatívnych predpisov v oblasti kybernetickej bezpečnosti. Zvýšenie produktivity: Zníženie výpadkov a porúch súvisiacich s kybernetickými útokmi.

Pre koho?

Školenie Manažér pre kybernetickú bezpečnosť MKB podľa NIS2 je určené pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za riadenie kybernetickej bezpečnosti v organizácii, s dôrazom na splnenie požiadaviek NIS2. IT profesionálov: Ktorí sa chcú špecializovať na oblasť kybernetickej bezpečnosti a implementáciu NIS2. Osoby zodpovedné za ochranu dát: V rámci organizácie s ohľadom na požiadavky NIS2. Audítorov informačných systémov: Ktorí sa chcú zamerať na audity kybernetickej bezpečnosti s ohľadom na NIS2. Každý, kto sa chce dozvedieť viac o riadení kybernetickej bezpečnosti v súlade s NIS2.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o kybernetickej bezpečnosti v kontexte NIS2: Školenie pokrýva širokú škálu tém relevantných pre riadenie kybernetickej bezpečnosti s ohľadom na požiadavky NIS2. Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty riadenia kybernetickej bezpečnosti a implementácie NIS2 a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi. Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti a zručnosti

ŠTANDARD PRE VÝROBCOV AUTOMOBILOV A ICH DODÁVATEĽOV ZALOŽENÝ NA ŠTANDARDE ISO 27001

Čo je?

Školenie TISAX Manažér pre informačnú bezpečnosť v automobilovom priemysle je komplexný program, ktorý rozvíja znalosti a zručnosti potrebné na efektívne riadenie informačnej bezpečnosti v súlade s požiadavkami TISAX (Trusted Information Security Assessment Exchange). TISAX je rámec pre hodnotenie informačnej bezpečnosti v automobilovom priemysle, ktorý definuje požiadavky na ochranu informácií a dát v dodávateľskom reťazci.

Prečo?

Absolvovanie školenia TISAX Manažér pre informačnú bezpečnosť prináša viacero benefitov:
Zvýšenie informačnej bezpečnosti: Získanie znalostí a zručností potrebných na efektívne riadenie informačnej bezpečnosti a zníženie rizika kybernetických útokov v súlade s požiadavkami TISAX.
Zníženie finančných strát: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadov šetrí finančné prostriedky. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k informačnej bezpečnosti a k dodržiavaniu požiadaviek TISAX posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu.
Zlepšenie súladu s regulačnými požiadavkami: Školenie sa zameriava na splnenie požiadaviek TISAX a relevantných legislatívnych predpisov v oblasti informačnej bezpečnosti. Zvýšenie produktivity: Zníženie výpadkov a porúch súvisiacich s kybernetickými útokmi.

Pre koho?

Školenie TISAX Manažér pre informačnú bezpečnosť v automobilovom priemysle je určené pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za riadenie informačnej bezpečnosti v organizácii, s dôrazom na splnenie požiadaviek TISAX. IT profesionálov: Ktorí sa chcú špecializovať na oblasť informačnej bezpečnosti a implementáciu TISAX. Osoby zodpovedné za ochranu dát: V rámci organizácie s ohľadom na požiadavky TISAX.
Audítorov informačných systémov: Ktorí sa chcú zamerať na audity informačnej bezpečnosti s ohľadom na TISAX. Každý, kto sa chce dozvedieť viac o riadení informačnej bezpečnosti v súlade s TISAX.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o informačnej bezpečnosti v kontexte TISAX: Školenie pokrýva širokú škálu tém relevantných pre riadenie informačnej bezpečnosti s ohľadom na požiadavky TISAX.
Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty riadenia informačnej bezpečnosti a implementácie TISAX a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi.
Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti a zručnosti v oblasti riadenia informačnej bezpečnosti v súlade s TISAX. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti informačnej bezpečnosti v automobilovom priemysle.

ŠKOLENIE NOVÁ NORMA ISO 27001:2022 PRINÁŠA REVOLUČNÚ ZMENU V RIADENÍ INFORMAČNEJ BEZPEČNOSTI

Čo je?

Školenie Nová norma ISO 27001:2022 je komplexný program, ktorý rozvíja znalosti a zručnosti relevantné pre implementáciu a údržbu systému riadenia informačnej bezpečnosti podľa novej verzie normy ISO 27001:2022. Školenie sa zameriava na rôzne aspekty normy, ako napríklad: Požiadavky normy: Podrobné pochopenie požiadaviek novej verzie normy ISO 27001:2022. Implementácia systému: Praktické kroky a nástroje na implementáciu systému riadenia informačnej bezpečnosti. Riadenie rizík: Identifikácia, analýza a hodnotenie rizík informačnej bezpečnosti v súlade s normou. Ochrana dát: Implementácia a dodržiavanie bezpečnostných opatrení na ochranu dát v súlade s normou. Audity a hodnotenia: Pochopenie procesov auditovania a hodnotenia systému riadenia informačnej bezpečnosti.

Prečo?

Absolvovanie školenia Nová norma ISO 27001:2022 prináša viacero benefitov:
Zvýšenie informačnej bezpečnosti: Získanie znalostí a zručností potrebných na efektívne riadenie informačnej bezpečnosti a zníženie rizika kybernetických útokov. Zníženie finančných strát: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadov šetrí finančné prostriedky. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k informačnej bezpečnosti a k dodržiavaniu medzinárodne uznávanej normy posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu. Zlepšenie súladu s regulačnými požiadavkami: Norma ISO 27001:2022 je v súlade s mnohými regulačnými požiadavkami v oblasti informačnej bezpečnosti. Zvýšenie produktivity: Zníženie výpadkov a porúch súvisiacich s kybernetickými útokmi.

Pre koho?

Školenie Nová norma ISO 27001:2022 je určené pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za riadenie informačnej bezpečnosti v organizácii.
IT profesionálov: Ktorí sa chcú špecializovať na oblasť informačnej bezpečnosti a implementáciu normy ISO 27001:2022.
Osoby zodpovedné za ochranu dát: V rámci organizácie. Audítorov informačných systémov: Ktorí sa chcú zamerať na audity informačnej bezpečnosti s ohľadom na normu ISO 27001:2022.
Každý, kto sa chce dozvedieť viac o riadení informačnej bezpečnosti podľa normy ISO 27001:2022.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o norme ISO 27001:2022: Školenie pokrýva širokú škálu tém relevantných pre implementáciu a údržbu systému riadenia informačnej bezpečnosti podľa novej verzie normy.
Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty implementácie a údržby systému riadenia informačnej bezpečnosti a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi.
Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti a zručnosti v oblasti riadenia informačnej bezpečnosti podľa normy ISO 27001:2022. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti informačnej bezpečnosti.

NAKIB

ŠKOLENIA

Vykonávanie analýzy rizík

VYKONANIE ANALÝZY RIZÍK Z POHĽADU ICT PRE POTREBY INFORMAČNEJ ALEBO KYBER BEZPEČNOSTI, PRIVACY PRE VÝKON DPIA PODĽA GDPR ALEBO PROTIKORUPČNÉHO SYSTÉMU.

Čo je?

Školenie Vykonávanie analýzy rizík je komplexný program, ktorý rozvíja znalosti a zručnosti potrebné na efektívne identifikovanie, hodnotenie a riadenie rizík v rôznych kontextoch. Školenie sa zameriava na rôzne aspekty analýzy rizík, ako napríklad: Metódy analýzy: Pochopenie a používanie rôznych metód analýzy rizík, ako napríklad FMEA, HAZOP a SWOT. Identifikácia rizík: Systematická identifikácia potenciálnych rizík v rôznych oblastiach, ako napríklad v oblasti informačnej bezpečnosti, projektového manažmentu alebo v prevádzke.Hodnotenie rizík: Kvantifikácia a kvalifikácia rizík na základe ich pravdepodobnosti a dopadu. Riadenie rizík: Implementácia a monitorovanie stratégie riadenia rizík pre zníženie ich dopadu. Komunikácia o rizikách: Efektivna komunikácia o rizikách s manažmentom a ostatnými zainteresovanými stranami.

Prečo?

Absolvovanie školenia Vykonávanie analýzy rizík prináša viacero benefitov:
Zníženie rizík: Získanie znalostí a zručností potrebných na efektívnu identifikáciu a riadenie rizík, čím sa znižuje ich dopad na organizáciu. Zlepšenie rozhodovania: Analýza rizík umožňuje informovanejšie a efektívnejšie rozhodovanie v rôznych oblastiach. Zvýšenie efektivity: Riadenie rizík pomáha predchádzať problémom a zbytočným stratám. Zlepšenie súladu s regulačnými požiadavkami: Mnoho regulačných požiadaviek vyžaduje od organizácií implementáciu systému riadenia rizík. Zvýšenie konkurencieschopnosti: Schopnosť efektívne riadiť riziká je dôležitou súčasťou konkurencieschopnosti v dnešnom dynamickom prostredí.

Pre koho?

Školenie Vykonávanie analýzy rizík je určené pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za riadenie rizík v organizácii.
Projektových manažérov: Ktorí potrebujú efektívne riadiť riziká v projektoch.
IT profesionálov: Ktorí sa chcú špecializovať na oblasť riadenia rizík.
Audítorov: Ktorí sa chcú zamerať na audity riadenia rizík.
Každý, kto sa chce dozvedieť viac o analýze a riadení rizík.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o analýze a riadení rizík: Školenie pokrýva širokú škálu tém relevantných pre efektívne riadenie rizík. Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty analýzy a riadenia rizík a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi. Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti a zručnosti v oblasti analýzy a riadenia rizík. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti riadenia rizík.

NAKIB

ŠKOLENIA

Manažér pre riadenie kontinuity činností

RIADENIE BCM PODĽA ISO 22301 A ISO 22313. VYKONANIE ANALÝZY OBCHODNÉHO DOPADU PODĽA ISO 22317, PRÍPRAVA A TESTOVANIE PLÁNOV OBNOVY

Čo je?

Školenie Manažér pre riadenie kontinuity činností je komplexný program, ktorý rozvíja znalosti a zručnosti potrebné na efektívne riadenie kontinuity činností v organizácii. Školenie sa zameriava na rôzne aspekty riadenia kontinuity činností, ako napríklad: Identifikácia rizík: Rozpoznanie a analýza rizík, ktoré by mohli narušiť chod organizácie. Plánovanie kontinuity: Vytváranie a implementácia plánu kontinuity činností, ktorý zaistí fungovanie organizácie aj v prípade neočakávaných udalostí. Testovanie a cvičenie plánu: Pravidelné testovanie a cvičenie plánu kontinuity činností pre zaistenie jeho efektívnosti. Komunikácia a koordinácia: Zaistenie efektívnej komunikácie a koordinácie medzi rôznymi oddeleniami a zainteresovanými stranami v rámci riadenia kontinuity činností. Udržiavanie a aktualizácia plánu: Pravidelné aktualizácie plánu kontinuity činností v súlade s aktuálnymi podmienkami a potrebami organizácie.

Prečo?

Absolvovanie školenia Manažér pre riadenie kontinuity činností prináša viacero benefitov:
Zvýšenie odolnosti organizácie: Získanie znalostí a zručností potrebných na efektívne riadenie kontinuity činností a zaistenie fungovania organizácie aj v prípade neočakávaných udalostí. Zníženie finančných strát: Predchádzanie a minimalizácia dopadov výpadkov a narušení chodu organizácie. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k kontinuite činností posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu. Zlepšenie súladu s regulačnými požiadavkami: Mnoho regulačných požiadaviek vyžaduje od organizácií implementáciu systému riadenia kontinuity činností. Zvýšenie produktivity: Zníženie prestojov a rýchle obnovenie chodu organizácie po neočakávaných udalostiach.

Pre koho?

Školenie Manažér pre riadenie kontinuity činností je určené pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za riadenie kontinuity činností v organizácii. IT profesionálov: Ktorí sa chcú špecializovať na oblasť riadenia kontinuity činností. Osoby zodpovedné za krízové manažment: V rámci organizácie. Audítorov: Ktorí sa chcú zamerať na audity riadenia kontinuity činností. Každý, kto sa chce dozvedieť viac o riadení kontinuity činností.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o riadení kontinuity činností: Školenie pokrýva širokú škálu tém relevantných pre efektívne riadenie kontinuity činností. Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty riadenia kontinuity činností a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi. Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti a zručnosti v oblasti riadenia kontinuity činností. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti riadenia kontinuity činností.

APLIKOVANIE ZÁKONA O ITVS, BEZPEČNOSTNÝ PROJEKT, ZÁKLADY SDLC, VYKONANIE ANALÝZY RIZÍK

Čo je?

Školenie Znalosti Zákona o informačných technológiách vo verejnej správe 95/2019 je komplexný program, ktorý rozvíja znalosti a zručnosti relevantné pre pochopenie a dodržiavanie Zákona o informačných technológiách vo verejnej správe (ZITVS) č. 95/2019 Z. z. Školenie sa zameriava na rôzne aspekty ZITVS, ako napríklad: Povinnosti a práva: Pochopenie povinností a práv verejných subjektov v súvislosti s informačnými technológiami. Informačné systémy: Kategorizácia a riadenie informačných systémov vo verejnej správe. Kybernetická bezpečnosť: Implementácia a dodržiavanie bezpečnostných opatrení v súlade s ZITVS. Ochrana osobných údajov: Pochopenie a dodržiavanie GDPR v kontexte ZITVS. Elektronické služby: Poskytovanie elektronických služieb verejnej správy v súlade s ZITVS. Zadávanie zákaziek: Pochopenie procesov zadávania zákaziek na informačné technológie vo verejnej správe.

Prečo?

Absolvovanie školenia Znalosti Zákona o informačných technológiách vo verejnej správe 95/2019 prináša viacero benefitov: Zvýšenie informovanosti: Získanie komplexného prehľadu o požiadavkách ZITVS a relevantných legislatívnych predpisov. Zníženie rizík: Predchádzanie sankciám a pokutám za nedodržiavanie ZITVS. Zvýšenie efektivity: Zlepšenie riadenia informačných technológií vo verejnej správe.Zvýšenie kybernetickej bezpečnosti: Posilnenie ochrany informačných systémov a dát pred kybernetickými hrozbami. Zlepšenie kvality elektronických služieb: Poskytovanie kvalitných a dostupných elektronických služieb pre občanov.

Pre koho?

Školenie Znalosti Zákona o informačných technológiách vo verejnej správe 95/2019 je určené pre: Zamestnancov verejnej správy: Ktorí sa podieľajú na riadení informačných technológií, kybernetickej bezpečnosti, ochrane osobných údajov, či poskytovaní elektronických služieb. Vedúcich pracovníkov: Zodpovedných za dodržiavanie ZITVS v rámci svojej organizačnej jednotky. IT profesionálov: Ktorí sa chcú špecializovať na oblasť informačných technológií vo verejnej správe. Právnikov: Ktorí sa venujú právnym aspektom informačných technológií a verejnej správy. Každý, kto sa chce dozvedieť viac o ZITVS a jeho dopade na verejnú správu.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy: Získanie komplexného prehľadu o ZITVS: Školenie pokrýva širokú škálu tém relevantných pre pochopenie a dodržiavanie ZITVS. Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty implementácie ZITVS a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi. Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti o ZITVS. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti informačných technológií vo verejnej správe.

NAKIB

ŠKOLENIA

Požiadavky v oblasti ochrany OÚ GDPR

POŽIADAVKY EU REGULÁCIE PRE OCHRANU OSOBNÝCH ÚDAJOV PODĽA GDPR NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679

Čo je?

Školenie Požiadavky v oblasti ochrany osobných údajov v zmysle požiadaviek nariadenia GDPR je komplexný program, ktorý rozvíja znalosti a zručnosti relevantné pre pochopenie a dodržiavanie GDPR (General Data Protection Regulation). Školenie sa zameriava na rôzne aspekty GDPR, ako napríklad: Základné pojmy: Definícia a pochopenie kľúčových pojmov GDPR ako sú osobné údaje, dotknutá osoba, prevádzkovateľ, sprostredkovateľ, súhlas a podobne.Povinnosti prevádzkovateľa: Pochopenie a implementácia povinností prevádzkovateľa v súvislosti so spracovaním osobných údajov, ako sú princípy spracovania, práva dotknutej osoby, technické a organizačné opatrenia a podobne. Práva dotknutej osoby: Pochopenie a implementácia práv dotknutej osoby, ako je právo na prístup k informáciám, právo na opravu, právo na vymazanie a podobne. Spracovanie osobných údajov: Praktické aspekty spracovania osobných údajov v rôznych kontextoch, ako je napríklad spracovanie osobných údajov v marketingu, v e-shope, v kamerovom systéme a podobne. Dokumentačné povinnosti: Pochopenie a implementácia dokumentačných povinností prevádzkovateľa, ako je vedenie záznamov o spracovateľských činnostiach, posudzovanie vplyvu na ochranu osobných údajov a podobne. Sankcie: Pochopenie a prevencia sankcií za porušenie GDPR.

Prečo?

Absolvovanie školenia Požiadavky v oblasti ochrany osobných údajov v zmysle požiadaviek nariadenia GDPR prináša viacero benefitov: Zvýšenie informovanosti: Získanie komplexného prehľadu o požiadavkach GDPR a relevantných legislatívnych predpisov. Zníženie rizík: Predchádzanie sankciám a pokutám za nedodržiavanie GDPR. Posilnenie dôvery: Demonštrovanie záväzku k ochrane osobných údajov a budovanie dôvery klientov, partnerov a regulačných orgánov. Zlepšenie reputácie: Prezentácia organizácie ako zodpovednej a transparentnej v oblasti ochrany osobných údajov. Zvýšenie efektivity: Zlepšenie procesov spracovania osobných údajov a minimalizácia administratívnej záťaže.

Pre koho?

Školenie Požiadavky v oblasti ochrany osobných údajov v zmysle požiadaviek nariadenia GDPR je určené pre: Zamestnancov: Ktorí sa podieľajú na spracovaní osobných údajov v rôznych oddeleniach, ako napríklad v marketingu, v HR, v IT, v obchodnom oddelení a podobne. Vedúcich pracovníkov: Zodpovedných za dodržiavanie GDPR v rámci svojej organizačnej jednotky.Manažérov: Ktorí potrebujú strategický prehľad o GDPR a jeho dopade na fungovanie organizácie. IT profesionálov: Ktorí sa chcú špecializovať na oblasť ochrany osobných údajov. Právnikov: Ktorí sa venujú právnym aspektom ochrany osobných údajov. Každý, kto sa chce dozvedieť viac o GDPR a jeho dopade na jednotlivcov a organizácie.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o GDPR: Školenie pokrýva širokú škálu tém relevantných pre pochopenie a dodržiavanie GDPR. Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty implementácie GDPR a umožňuje účastníkom aplikovať nadobudnuté znalosti.

ZÁKLADNÉ TECHNIKY HACKERSKÝCH ÚTOKOV

Čo je?

Školenie Základy hackingu je komplexný program, ktorý rozvíja znalosti a zručnosti relevantné pre pochopenie a simuláciu techník používaných hackermi. Školenie sa zameriava na rôzne aspekty hackingu, ako napríklad: Typy hackerov: Úvod do rôznych typov hackerov a ich motívov. Metódy hackovania: Pochopenie a simulácia rôznych metód hackovania, ako sú phishing, social engineering, SQL injection, XSS a podobne. Sieťová bezpečnosť: Základy sieťovej bezpečnosti a zraniteľnosti, ako napríklad sniffing, spoofing, denial-of-service attacks a podobne. Penetračné testovanie: Úvod do penetračného testovania a jeho využitia pri identifikácii a zmierňovaní zraniteľností. Bezpečnosť webu: Zraniteľnosti webových aplikácií a metódy ich zneužitia. Kryptografia: Základy kryptografie a jej využitie pri ochrane dát. Etika hackingu: Dôležitosť etického prístupu k hackingu a zodpovedného používania získaných znalostí.

Prečo?

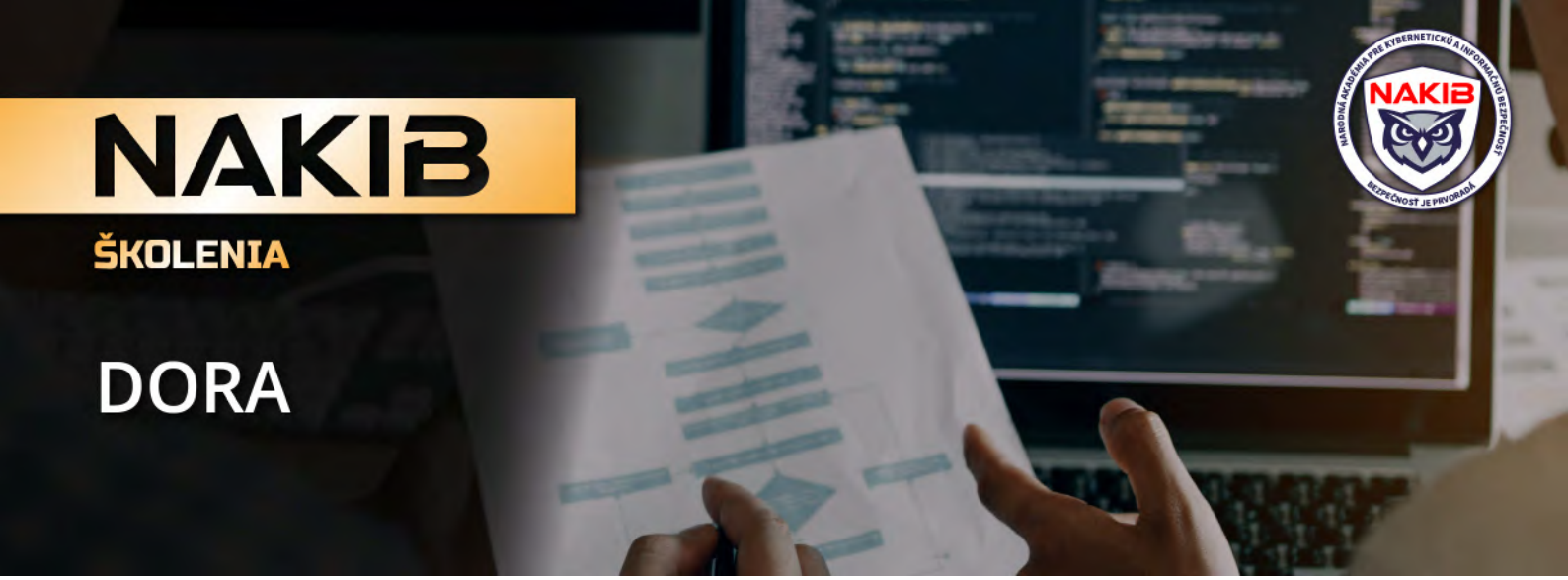
Absolvovanie školenia Základy hackingu prináša viacero benefitov:
Zvýšenie povedomia o kybernetických hrozbách: Získanie komplexného prehľadu o rôznych technikách hackovania a metódach ochrany pred nimi. Zlepšenie kybernetickej bezpečnosti: Posilnenie obranyschopnosti organizácie voči kybernetickým útokom. Rozvoj analytických a logických zručností: Tréning v identifikácii a riešení bezpečnostných zraniteľností. Zvýšenie kariérnych príležitostí: Získanie znalostí a zručností relevantných pre rôzne profesie v oblasti kybernetickej bezpečnosti. Posilnenie pocitu kontroly: Získanie nástrojov a techník na ochranu osobných dát a zariadení pred hackermi.

Pre koho?

Školenie Základy hackingu je určené pre:
IT profesionálov: Ktorí sa chcú špecializovať na oblasť kybernetickej bezpečnosti.
Začínajúcich hackerov: Ktorí sa chcú eticky naučiť techniky používané hackermi.
Študentov informatiky: Ktorí sa chcú dozvedieť viac o kybernetických hrozbách a ich riešení.
Manažérov a vedúcich pracovníkov: Zodpovedných za kybernetickú bezpečnosť v organizácii.
Každý, kto sa chce dozvedieť viac o hackingu a ochrane pred ním.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o hackingu: Školenie pokrýva širokú škálu tém relevantných pre pochopenie rôznych techník hackovania. Rozvoj praktických zručností: Školenie sa zameriava na simuláciu techník hackovania v bezpečnom prostredí a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi.
Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti o hackingu. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti kybernetickej bezpečnosti.



PORADENSTVO V OBLASTI PRÍPRAVY NA MEDZINÁRODNÉHO ŠTANDARDU DORA PRE FINANČNÉ SLUŽBY

Čo je?

Školenie DORA (Digital Operational Resilience Act) je komplexný program, ktorý rozvíja znalosti a zručnosti relevantné pre implementáciu a dodržiavanie nariadenia DORA o digitálnej prevádzkovej odolnosti. Školenie sa zameriava na rôzne aspekty DORA, ako napríklad: Požiadavky nariadenia: Podrobné pochopenie požiadaviek nariadenia DORA, vrátane definície kľúčových pojmov, identifikovaných rizík a povinností regulovaných subjektov. Riadenie rizík ICT: Implementácia a udržiavanie efektívneho systému riadenia rizík v oblasti informačných a komunikačných technológií (ICT) v súlade s DORA. Incident manažment: Pochopenie a implementácia procesov riadenia incidentov ICT v súlade s požiadavkami DORA. Testovanie odolnosti: Plánovanie a realizácia testovania odolnosti ICT infraštruktúry a systémov v súlade s DORA. Dohľad a reporting: Pochopenie a dodržiavanie požiadaviek na dohľad a reporting v súvislosti s DORA. Technické aspekty: Praktické znalosti o technických riešeniach relevantných pre implementáciu DORA, ako napríklad cloudové technológie.

Prečo?

Absolvovanie školenia DORA prináša viacero benefitov:
Zvýšenie odolnosti voči ICT hrozbám: Získanie znalostí a zručností potrebných na efektívne riadenie rizík a budovanie odolnosti voči ICT hrozbám v súlade s DORA. Zníženie rizika sankcií: Predchádzanie sankciám za nedodržiavanie nariadenia DORA. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k digitálnej prevádzkovej odolnosti a budovanie dôvery klientov, partnerov a regulačných orgánov. Zlepšenie súladu s regulačnými požiadavkami: DORA nadväzuje na existujúce regulačné požiadavky v oblasti ICT a jej implementácia prispieva k celkovému súladu. Zvýšenie efektivity a produktivity: Zníženie prestojov a výpadkov ICT systémov a zlepšenie celkovej efektivity prevádzky.

Pre koho?

Školenie DORA je určené pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za implementáciu a dodržiavanie DORA v rámci svojej organizačnej jednotky. IT profesionálov: Ktorí sa podieľajú na riadení ICT rizík, incidente manažmente, testovaní odolnosti a dodržiavaní požiadaviek DORA. Audítorov: Ktorí sa chcú zamerať na audity DORA a digitálnej prevádzkovej odolnosti. Právnikov: Ktorí sa venujú právnym aspektom DORA a regulácie ICT. Každý, kto sa chce dozvedieť viac o DORA a jej dopade na rôzne sektory.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o DORA: Školenie pokrýva širokú škálu tém relevantných pre pochopenie a implementáciu nariadenia DORA. Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty implementácie DORA a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi. Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti o DORA. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti digitálnej prevádzkovej odolnosti.

ŠKOLENIE O APLIKOVANÍ ZÁKONA O UTAJOVANÝCH SKUTOČNOSTIACH 215/2004

Čo je?

Školenie Zákon o utajovaných skutočnostiach 215/2004 Z. z.
Čo to znamená: Školenie Zákon o utajovaných skutočnostiach 215/2004 Z. z. (ZUOS) je komplexný program, ktorý rozvíja znalosti a zručnosti relevantné pre pochopenie a dodržiavanie ZUOS. Školenie sa zameriava na rôzne aspekty ZUOS, ako napríklad: Definícia utajovanej skutočnosti: Pochopenie a identifikácia informácií a vecí, ktoré sa považujú za utajované v súlade s ZUOS. Stupne utajenia: Rozlišovanie medzi rôznymi stupňami utajenia (prísne tajné, tajné, chránené) a ich dopad na manipuláciu s utajovanými skutočnosťami. Povinnosti a práva: Pochopenie a dodržiavanie povinností a práv subjektov, ktoré prichádzajú do styku s utajovanými skutočnosťami. Manipulácia s utajovanými skutočnosťami: Praktické aspekty nakladania s utajovanými informáciami a materiálmi, ako napríklad ich spracovanie, uchovávanie, prenos a likvidácia. Ochrana utajovaných skutočností: Implementácia bezpečnostných opatrení na ochranu utajovaných skutočností pred neoprávneným zneužitím, vyzradením alebo poškodením. Dohľad a sankcie: Pochopenie systému dohľadu nad dodržiavaním ZUOS a sankcií za jeho porušenie.

Prečo?

Absolvovanie školenia Zákon o utajovaných skutočnostiach 215/2004 Z. z. prináša viacero benefitov:
Zvýšenie informovanosti: Získanie komplexného prehľadu o požiadavkách ZUOS a relevantných legislatívnych predpisov. Zníženie rizík: Predchádzanie sankciám a pokutám za nedodržiavanie ZUOS. Ochrana citlivých informácií: Zabezpečenie ochrany utajovaných informácií a materiálov pred neoprávneným prístupom. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k ochrane utajovaných informácií a budovanie dôvery klientov, partnerov a regulačných orgánov. Zvýšenie efektivity: Zlepšenie procesov manipulácie s utajovanými informáciami a minimalizácia administratívnej záťaže.

Pre koho?

Školenie Zákon o utajovaných skutočnostiach 215/2004 Z. z. je určené pre:
Zamestnancov: Ktorí prichádzajú do styku s utajovanými informáciami a materiálmi v rôznych oddeleniach, ako napríklad v štátnej správe, v armáde, v bezpečnostných zložkách, v strategických podnikoch a podobne. Vedúcich pracovníkov: Zodpovedných za dodržiavanie ZUOS v rámci svojej organizačnej jednotky. Manažérov informačnej bezpečnosti: Ktorí sa podieľajú na implementácii a udržiavaní systému ochrany utajovaných informácií. Právnikov: Ktorí sa venujú právnym aspektom ochrany utajovaných informácií. Každý, kto sa chce dozvedieť viac o ZUOS a jeho dopade na rôzne sektory.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o ZUOS: Školenie pokrýva širokú škálu tém relevantných pre pochopenie a dodržiavanie ZUOS. Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty implementácie ZUOS a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi. Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti o ZUOS. Networking: Školenie umožňuje účastníkom nadviazať kontakt s ostatnými profesionálmi z rôznych oblastí.

ŠKOLENIE O VYUŽÍVANÍ AI – UMELEJ INTELIGENCIE V PRAXI

Čo je?

Školenie AI - Umelá inteligencia je komplexný program, ktorý rozvíja znalosti a zručnosti relevantné pre pochopenie a využitie umelej inteligencie (AI) v rôznych oblastiach. Školenie sa zameriava na rôzne aspekty AI, ako napríklad: Základné pojmy: Definícia a pochopenie kľúčových pojmov AI, ako sú strojové učenie, hlboké učenie, neurónové siete, algoritmy a podobne. Typy AI: Rozdelenie AI na rôzne typy (reaktívna, limitovaná pamäťou, teória mysle), ich vlastnosti a príklady využitia. Využitie AI: Praktické aplikácie AI v rôznych sektoroch, ako napríklad v medicíne, financiách, marketingu, výrobe, doprave a podobne. Etické aspekty: Dôležitosť etického prístupu k AI a zodpovedného používania jej technológií. Budúcnosť AI: Trendy a očakávaný vývoj v oblasti AI v najbližších rokoch.

Prečo?

Absolvovanie školenia AI - Umelá inteligencia prináša viacero benefitov:
Zvýšenie informovanosti: Získanie komplexného prehľadu o rôznych aspektoch AI a jej potenciáli. Zlepšenie konkurencieschopnosti: Získanie znalostí a zručností potrebných pre implementáciu a využitie AI v rôznych oblastiach a posilnenie konkurencieschopnosti na trhu. Zvýšenie efektivity: Automatizácia a optimalizácia procesov pomocou AI a zníženie administratívnej záťaže. Inovácia: Podpora inovatívnych riešení a produktov s využitím AI. Zlepšenie rozhodovania: Využitie AI pre analýzu dát a podporu informovaného a strategického rozhodovania.

Pre koho?

Školenie AI - Umelá inteligencia je určené pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za strategické plánovanie a implementáciu AI v rámci svojej organizačnej jednotky. IT profesionálov: Ktorí sa chcú špecializovať na oblasť AI a strojového učenia. Podnikateľov: Ktorí chcú využiť AI pre rast a inováciu svojho podnikania. Študentov informatiky: Ktorí sa chcú dozvedieť viac o AI a jej potenciálnom využití v praxi. Každý, kto sa chce dozvedieť viac o AI a jej dopade na rôzne sektory.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o AI: Školenie pokrýva širokú škálu tém relevantných pre pochopenie rôznych aspektov AI. Rozvoj praktických zručností: Školenie sa zameriava na praktické aplikácie AI a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi. Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti o AI. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti AI.

ŠPECIFICKÝ PRÍSTUP RIADENIA INFORMAČNEJ A KYBERNETICKEJ BEZPEČNOSTI VO VÝROBNÝCH SPOLOČNOSTIACH

Čo je?

Školenie Kybernetická bezpečnosť v OT prostredí je komplexný program, ktorý rozvíja znalosti a zručnosti relevantné pre ochranu operačných technológií (OT) pred kybernetickými hrozbami. Školenie sa zameriava na rôzne aspekty kybernetickej bezpečnosti v OT prostredí, ako napríklad: Základné pojmy: Definícia a pochopenie kľúčových pojmov kybernetickej bezpečnosti v OT prostredí, ako sú SCADA systémy, ICS systémy, hrozby, zraniteľnosti a riziká. Typy kybernetických hrozieb: Rozdelenie kybernetických hrozieb relevantných pre OT prostredie (malware, phishing, DDoS útoky, zero-day útoky) a ich dopad na OT systémy. Ochrana OT infraštruktúry: Implementácia a udržiavanie bezpečnostných opatrení pre OT infraštruktúru, ako napríklad sieťová segmentácia, firewally, autentifikácia a autorizácia. Riadenie rizík: Identifikácia, analýza a riadenie rizík kybernetickej bezpečnosti v OT prostredí. Incident manažment: Pochopenie a implementácia procesov riadenia incidentov kybernetickej bezpečnosti v OT prostredí. Dodržiavanie regulácií: Pochopenie a dodržiavanie regulačných požiadaviek na kybernetickú bezpečnosť v OT prostredí.

Prečo?

Absolvovanie školenia Kybernetická bezpečnosť v OT prostredí prináša viacero benefitov:
Zvýšenie informovanosti: Získanie komplexného prehľadu o kybernetických hrozbách a rizikách v OT prostredí.
Zníženie rizík: Predchádzanie kybernetickým útokom a minimalizácia ich dopadu na OT systémy a prevádzku. Zvýšenie odolnosti: Posilnenie odolnosti OT infraštruktúry voči kybernetickým hrozbám. Zabezpečenie kontinuity prevádzky: Zníženie prestojov a výpadkov OT systémov v dôsledku kybernetických útokov. Dodržiavanie regulácií: Zabezpečenie súladu s regulačnými požiadavkami na kybernetickú bezpečnosť v OT prostredí.

Pre koho?

Školenie Kybernetická bezpečnosť v OT prostredí je určené pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za kybernetickú bezpečnosť v OT prostredí.
IT profesionálov: Ktorí sa podieľajú na správe a zabezpečení OT infraštruktúry.
Prevádzkových inžinierov: Ktorí pracujú s OT systémami a zariadeniami.
Audítorov: Ktorí sa venujú auditu kybernetickej bezpečnosti v OT prostredí.
Každý, kto sa chce dozvedieť viac o kybernetickej bezpečnosti v OT prostredí.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o kybernetickej bezpečnosti v OT prostredí: Školenie pokrýva širokú škálu tém relevantných pre pochopenie a riešenie kybernetických hrozieb v OT prostredí.
Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty kybernetickej bezpečnosti v OT prostredí a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi. Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti o kybernetickej bezpečnosti v OT prostredí. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti kybernetickej bezpečnosti v OT prostredí.

NAKIB

AUDIT A GAP ANALÝZY

NAKIB.SK

VYKONANIE AUDITU ALEBO GAP ANALÝZY PODĽA POŽIADAVIEK CYBER SECURITY 69/2018 ZOKB

Čo je?

Výkon auditu Cyber security je komplexný proces posudzovania súladu informačného systému a kybernetickej bezpečnosti organizácie s požiadavkami Cyber security zákona a jeho vyhlášok. Audit zahŕňa: Analýzu rizík: Identifikácia a hodnotenie rôznych typov rizík kybernetických hrozieb a zraniteľností informačného systému. Posúdenie bezpečnostných opatrení: Hodnotenie existujúcich bezpečnostných opatrení organizácie a ich súladu s požiadavkami Cyber security zákona. Testovanie penetrácie: Simulácia kybernetických útokov s cieľom identifikovať a preveriť zraniteľnosti informačného systému. Vypracovanie správy: Zhrnutie zistení auditu a odporúčaní na zlepšenie kybernetickej bezpečnosti.

Prečo?

Zavedenie auditu Cyber security prináša viacero benefitov:
Zvýšenie súladu: Zabezpečenie súladu s požiadavkami Cyber security zákona a zníženie rizika sankcií. Zníženie rizík: Zvýšenie kybernetickej bezpečnosti a zníženie rizika kybernetických incidentov. Zlepšenie reputácie: Preukázanie záväzku k kybernetickej bezpečnosti posilňuje dôveru partnerov a zákazníkov. Zvýšenie konkurencieschopnosti: Dobre chránený informačný systém môže priniesť organizácii konkurenčnú výhodu.

Pre koho?

Audit Cyber security je určený pre:
Všetky organizácie: Bez ohľadu na veľkosť alebo typ činnosti, ktoré spracúvajú chránené údaje v súlade s Cyber security zákonom. Organizácie, ktoré chcú zlepšiť kybernetickú bezpečnosť: Audit môže identifikovať oblasti, v ktorých je možné zlepšiť kybernetickú bezpečnosť a znížiť riziká. Organizácie, ktoré sa chystajú na certifikáciu kybernetickej bezpečnosti: Audit môže pomôcť organizácii pripraviť sa na certifikáciu podľa medzinárodných štandardov.

Prínosy?

Implementácia auditu Cyber security prináša nasledovné prínosy:
Zvýšenie povedomia o kybernetických hrozbách a rizikách: Audit môže pomôcť manažmentu a zamestnancom uvedomiť si dôležitosť kybernetickej bezpečnosti a potenciálne dopady kybernetických incidentov. Zlepšenie bezpečnostných procesov a opatrení: Audit môže identifikovať oblasti, v ktorých je možné zlepšiť bezpečnostné procesy a opatrenia a implementovať relevantné kontroly v súlade s Cyber security zákonom. Zníženie rizika kybernetických incidentov: Včasná identifikácia a náprava zraniteľností informačného systému môže znížiť riziko kybernetických incidentov a minimalizovať ich dopady.
Zvýšenie dôvery partnerov a zákazníkov: Preukázanie záväzku k kybernetickej bezpečnosti a súladu s Cyber security zákonom posilňuje dôveru partnerov a zákazníkov v organizáciu.

VYKONANIE AUDITU ALEBO GAP ANALÝZY PODĽA POŽIADAVIEK CYBER SECURITY NIS

Čo je?

Výkon auditu Cyber security podľa Smernice NIS (NIS Directive)
Čo to znamená: Výkon auditu Cyber security podľa Smernice NIS (Directive on measures for a high common level of cybersecurity across the Union, známa aj ako NIS Directive) je komplexný proces posudzovania súladu informačného systému a kybernetickej bezpečnosti organizácie s požiadavkami Smernice NIS a jej transpozičného zákona v SR. Audit zahŕňa: Analýzu rizík: Identifikácia a hodnotenie rôznych typov rizík kybernetických hrozieb a zraniteľností informačného systému v kontexte požiadaviek Smernice NIS. Posúdenie bezpečnostných opatrení: Hodnotenie existujúcich bezpečnostných opatrení organizácie a ich súladu s požiadavkami Smernice NIS a transpozičného zákona. Testovanie penetrácie: Simulácia kybernetických útokov s cieľom identifikovať a preveriť zraniteľnosti informačného systému v súlade s metodikou testovania definovanou v Smernici NIS. Vypracovanie správy: Zhrnutie zistení auditu a odporúčaní na zlepšenie kybernetickej bezpečnosti s ohľadom na požiadavky Smernice NIS.

Prečo?

Zavedenie auditu Cyber security podľa Smernice NIS prináša viacero benefitov:
Zvýšenie súladu: Zabezpečenie súladu s požiadavkami Smernice NIS a transpozičného zákona v SR, čím sa minimalizuje riziko sankcií a administratívnych pokút. Zníženie rizík: Zvýšenie kybernetickej bezpečnosti a zníženie rizika kybernetických incidentov s ohľadom na špecifické hrozby a riziká definované v Smernici NIS. Zlepšenie reputácie: Preukázanie záväzku k kybernetickej bezpečnosti a súladu s reguláciou posilňuje dôveru partnerov, zákazníkov a orgánov dozoru. Zvýšenie konkurencieschopnosti: Dobre chránený informačný systém v súlade s požiadavkami Smernice NIS môže priniesť organizácii konkurenčnú výhodu.

Pre koho?

Audit Cyber security podľa Smernice NIS je určený pre:
Organizácie pôsobiace v tzv. “kľúčových sektoroch”: Energetika, doprava, bankovníctvo, financie, zdravie, digitálna infraštruktúra a verejná správa, ktoré spadajú pod pôsobnosť Smernice NIS a transpozičného zákona. Organizácie, ktoré chcú zlepšiť kybernetickú bezpečnosť: Audit môže identifikovať oblasti, v ktorých je možné zlepšiť kybernetickú bezpečnosť a znížiť riziká v kontexte požiadaviek Smernice NIS. Organizácie, ktoré sa chystajú na certifikáciu kybernetickej bezpečnosti: Audit môže pomôcť organizácii pripraviť sa na certifikáciu podľa medzinárodných štandardov s ohľadom na špecifiká Smernice NIS.

Prínosy?

Implementácia auditu Cyber security podľa Smernice NIS prináša nasledovné prínosy:
Zvýšenie povedomia o kybernetických hrozbách a rizikách relevantných pre kľúčové sektory: Audit sa zameriava na špecifické hrozby a riziká definované v Smernici NIS, čím zvyšuje povedomie manažmentu a zamestnancov v daných oblastiach. Zlepšenie bezpečnostných procesov a opatrení v súlade s požiadavkami Smernice NIS: Audit identifikuje oblasti, v ktorých je nutné implementovať alebo upraviť bezpečnostné opatrenia a procesy tak, aby spĺňali požiadavky Smernice NIS a transpozičného zákona. Zníženie rizika kybernetických incidentov a dopadov na kľúčové sektory: Včasná identifikácia a náprava zraniteľností informačného systému v súlade s metodikou Smernice NIS znižuje riziko kybernetických incidentov a minimalizuje ich dopady na prevádzku a služby.

VYKONANIE AUDITU ALEBO GAP ANALÝZY PODĽA POŽIADAVIEK ZÁKONA ITVS 95/2019 A VYHLÁŠKY 179/2020

Čo je?

Výkon auditu Verejná správa ITVS je komplexný proces posudzovania súladu informačného systému a IT infraštruktúry orgánu verejnej správy s požiadavkami Metodiky ITVS (Informačno-technické výstupy štandardu). Audit zahŕňa:
Analýzu rizík: Identifikácia a hodnotenie rôznych typov rizík kybernetických hrozieb a zraniteľností informačného systému a IT infraštruktúry v kontexte požiadaviek Metodiky ITVS.
Posúdenie súladu: Hodnotenie súladu informačného systému a IT infraštruktúry s požiadavkami Metodiky ITVS v oblastiach ako sú: riadenie IT, informačná bezpečnosť, riadenie prevádzky IT, riadenie zmien a vývoja IT a riadenie kontinuity IT. Testovanie penetrácie: Simulácia kybernetických útokov s cieľom identifikovať a preveriť zraniteľnosti informačného systému a IT infraštruktúry v súlade s metodikou testovania definovanou v Metodike ITVS.
Vypracovanie správy: Zhrnutie zistení auditu a odporúčaní na zlepšenie súladu s Metodikou ITVS a posilnenie kybernetickej bezpečnosti.

Prečo?

Zavedenie auditu Verejná správa ITVS prináša viacero benefitov:
Zvýšenie súladu: Zabezpečenie súladu s požiadavkami Metodiky ITVS, čím sa minimalizuje riziko sankcií a administratívnych pokút zo strany Úradu podpredsedu vlády SR pre informatizáciu a investície.
Zníženie rizík: Zvýšenie kybernetickej bezpečnosti a zníženie rizika kybernetických incidentov vďaka identifikácii a náprave zraniteľností v súlade s Metodikou ITVS. Zlepšenie efektivity a hospodárnosti IT: Implementácia odporúčaní z auditu môže priniesť optimalizáciu IT procesov a zníženie nákladov na prevádzku IT.
Zvýšenie transparentnosti a dôveryhodnosti: Preukázanie záväzku k transparentnosti a súladu s Metodikou ITVS posilňuje dôveru verejnosti v orgány verejnej správy.

Pre koho?

Audit Verejná správa ITVS je určený pre:
Všetky orgány verejnej správy: Vládne úrady, miestne samosprávy, štátne fondy a iné subjekty verejnej správy, ktoré sú povinné implementovať Metodiku ITVS. Organizácie, ktoré chcú zlepšiť kybernetickú bezpečnosť a súlad s Metodikou ITVS: Audit môže identifikovať oblasti, v ktorých je možné zlepšiť kybernetickú bezpečnosť a súlad s požiadavkami Metodiky ITVS. Organizácie, ktoré sa chystajú na certifikáciu kybernetickej bezpečnosti: Audit môže pomôcť orgánu verejnej správy pripraviť sa na certifikáciu podľa medzinárodných štandardov s ohľadom na špecifiká Metodiky ITVS.

Prínosy?

Implementácia auditu Verejná správa ITVS prináša nasledovné prínosy:
Zvýšenie povedomia o kybernetických hrozbách a rizikách relevantných pre verejnú správu: Audit sa zameriava na špecifické hrozby a riziká definované v Metodike ITVS, čím zvyšuje povedomie manažmentu a zamestnancov v daných oblastiach. Zlepšenie bezpečnostných procesov a opatrení v súlade s Metodikou ITVS: Audit identifikuje oblasti, v ktorých je nutné implementovať alebo upraviť bezpečnostné opatrenia a procesy tak, aby spĺňali požiadavky Metodiky ITVS. Zníženie rizika kybernetických incidentov a dopadov na chod procesov.

VYKONANIE GAP ANALÝZY PODĽA POŽIADAVIEK REGULÁCIE DORA PRE FINANČNÉ INŠTITÚCIE POD RIADENÍM NBS

Čo je?

Výkon GAP analýzy DORA (Digital Operational Resilience Act) je komplexný proces posudzovania súladu informačného systému a kybernetickej odolnosti organizácie s požiadavkami nariadenia DORA.
Audit zahŕňa: Analýzu rizík: Identifikácia a hodnotenie rôznych typov rizík prevádzkových výpadkov a kybernetických hrozieb v súlade s definíciou DORA. Posúdenie riadenia kybernetickej odolnosti: Hodnotenie existujúcich procesov a opatrení riadenia kybernetickej odolnosti v organizácii a ich súladu s požiadavkami DORA. Testovanie odolnosti: Simulácia rôznych scenárov prevádzkových výpadkov a kybernetických útokov s cieľom otestovať odolnosť informačného systému a reakcie organizácie. Vypracovanie správy: Zhrnutie zistení auditu a odporúčaní na zlepšenie kybernetickej odolnosti v súlade s nariadením DORA.

Prečo?

Vykonanie GAP analýzy DORA prináša viacero benefitov:
Zvýšenie súladu: Zabezpečenie súladu s požiadavkami nariadenia DORA, čím sa minimalizuje riziko sankcií a administratívnych pokút. Zníženie rizík: Zvýšenie kybernetickej odolnosti a zníženie rizika prevádzkových výpadkov a kybernetických incidentov. Zlepšenie kontinuity prevádzky: Implementácia odporúčaní z auditu môže posilniť kontinuitu prevádzky a minimalizovať dopady výpadkov a incidentov. Zvýšenie konkurencieschopnosti: Dobre chránený informačný systém a vysoká kybernetická odolnosť môže priniesť organizácii konkurenčnú výhodu.

Pre koho?

GAP analýza DORA je určená pre:
Finančné inštitúcie: Banky, poisťovne, investičné firmy a iné subjekty podliehajúce nariadeniu DORA. Poskytovateľov kritickej infraštruktúry: Prevádzkovatelia energetických sietí, telekomunikácií, dopravy a iných kritických sektorov definovaných v DORA. Organizácie, ktoré chcú zlepšiť kybernetickú odolnosť: Audit môže identifikovať oblasti, v ktorých je možné zlepšiť kybernetickú odolnosť a súlad s požiadavkami DORA. Organizácie, ktoré sa chystajú na certifikáciu kybernetickej odolnosti: Audit môže pomôcť organizácii pripraviť sa na certifikáciu podľa medzinárodných štandardov s ohľadom na špecifiká DORA.

Prínosy?

GAP analýzy DORA prináša nasledovné prínosy:
Preverenie úrovne súladu v oblastiach povedomia o rizikách prevádzkových výpadkov a kybernetických hrozieb: GAP analýzy DORA sa zameriava na špecifické hrozby a riziká definované v DORA.
Zlepšenie procesov a opatrení riadenia kybernetickej odolnosti: GAP analýzy DORA identifikuje oblasti, v ktorých je nutné implementovať alebo upraviť procesy a opatrenia riadenia kybernetickej odolnosti tak, aby spĺňali požiadavky DORA. Zníženie rizika prevádzkových výpadkov a kybernetických incidentov: Včasná identifikácia a náprava zraniteľností a slabín v kybernetickej odolnosti znižuje riziko a dopady výpadkov a incidentov. Posilnenie kontinuity prevádzkovej odolnosti.

VÝKON AUDITU ALEBO GAP ANALÝZY V OBLASTI ISMS (SYSTÉM RIADENIA INFORMAČNEJ BEZPEČNOSTI) PODĽA ISO 27001:2022

Čo je?

Výkon auditu ISO 27001 je komplexný proces posudzovania súladu systému manažmentu informačnej bezpečnosti (ISMS) organizácie s požiadavkami medzinárodnej normy ISO 27001. Audit zahŕňa:
Analýzu rizík: Identifikácia a hodnotenie rôznych typov rizík informačnej bezpečnosti v organizácii.
Posúdenie ISMS: Hodnotenie existujúcich procesov a opatrení ISMS a ich súladu s požiadavkami ISO 27001.
Testovanie kontrol: Testovanie vybraných kontrolných mechanizmov ISMS s cieľom overiť ich efektivitu.
Vypracovanie správy: Zhrnutie zistení auditu a odporúčaní na zlepšenie ISMS.

Prečo?

Zavedenie auditu ISO 27001 prináša viacero benefitov:
Zvýšenie súladu: Zabezpečenie súladu s požiadavkami ISO 27001, čím sa posilňuje dôvera partnerov a zákazníkov v organizáciu. Zníženie rizík: Zvýšenie informačnej bezpečnosti a zníženie rizika kybernetických incidentov. Zlepšenie procesov a opatrení: Implementácia odporúčaní z auditu môže optimalizovať procesy ISMS a zlepšiť celkovú informačnú bezpečnosť. Zvýšenie konkurencieschopnosti: Dobre chránený informačný systém a certifikácia ISO 27001 môže priniesť organizácii konkurenčnú výhodu.

Pre koho?

Audit ISO 27001 je určený pre:

Organizácie, ktoré chcú preukázať záväzok k informačnej bezpečnosti: Certifikácia ISO 27001 je medzinárodne uznávaným dôkazom o kvalite ISMS. Organizácie, ktoré chcú zlepšiť informačnú bezpečnosť: Audit môže identifikovať oblasti, v ktorých je možné zlepšiť ISMS a znížiť riziká. Organizácie, ktoré sa chystajú na certifikáciu ISO 27001: Audit môže pomôcť organizácii pripraviť sa na certifikačný proces.

Prínosy?

Implementácia auditu ISO 27001 prináša nasledovné prínosy:
Zvýšenie povedomia o informačnej bezpečnosti: Audit zvyšuje povedomie manažmentu a zamestnancov o dôležitosti informačnej bezpečnosti a ich zodpovednosti v rámci ISMS.
Zlepšenie procesov riadenia rizík: Audit podporuje systematický prístup k identifikácii, analýze a riadeniu rizík informačnej bezpečnosti. Zvýšenie efektivity a hospodárnosti ISMS: Implementácia odporúčaní z auditu môže priniesť optimalizáciu procesov ISMS a zníženie nákladov na informačnú bezpečnosť.
Posilnenie dôvery partnerov a zákazníkov: Certifikácia ISO 27001 preukazuje záväzok k informačnej bezpečnosti a posilňuje dôveru partnerov a zákazníkov v organizáciu.

VYKONANIE AUDITU ALEBO GAP ANALÝZY PODĽA POŽIADAVIEK BIZNIS KONTINUITY

Čo je?

Výkon auditu BCM (Business Continuity Management) je komplexný proces posudzovania súladu systému riadenia kontinuity prevádzky (BCMS) organizácie s požiadavkami normy ISO 22301 a osvedčených postupov BCM. Audit zahŕňa:
Analýzu rizík: Identifikácia a hodnotenie rôznych typov rizík prerušenia prevádzky a dopadov na kontinuitu biznisu.Posúdenie BCMS: Hodnotenie existujúcich procesov a opatrení BCMS a ich súladu s požiadavkami ISO 22301. Testovanie plánov kontinuity: Simulácia rôznych scenárov prerušenia prevádzky s cieľom overiť efektivitu plánov kontinuity a reakcie organizácie.Vypracovanie správy: Zhrnutie zistení auditu a odporúčaní na zlepšenie BCMS.

Prečo?

Zavedenie auditu BCM prináša viacero benefitov:
Zvýšenie súladu: Zabezpečenie súladu s požiadavkami ISO 22301, čím sa posilňuje dôvera partnerov a investorov v odolnosť organizácie. Zníženie rizík: Zvýšenie odolnosti voči prerušeniam prevádzky a minimalizácia dopadov na biznis. Zlepšenie procesov a plánov: Implementácia odporúčaní z auditu môže optimalizovať procesy BCMS a zdokonaliť plány kontinuity. Zvýšenie konkurencieschopnosti: Dobre pripravená organizácia na krízové scenáre a rýchle obnovenie prevádzky môže získať konkurenčnú výhodu.

Pre koho?

Audit BCM je určený pre:
Organizácie, ktoré chcú preukázať záväzok k riadeniu kontinuity prevádzky: Certifikácia ISO 22301 je medzinárodne uznávaným dôkazom o kvalite BCMS. Organizácie, ktoré chcú zlepšiť odolnosť voči prerušeniam prevádzky: Audit môže identifikovať oblasti, v ktorých je možné zlepšiť BCMS a znížiť riziká. Organizácie, ktoré sa chystajú na certifikáciu ISO 22301: Audit môže pomôcť organizácii pripraviť sa na certifikačný proces.

Prínosy?

mplementácia auditu BCM prináša nasledovné prínosy:
Zvýšenie povedomia o rizikách a dôležitosti kontinuity prevádzky: Audit zvyšuje povedomie manažmentu a zamestnancov o rizikách prerušenia prevádzky a ich zodpovednosti v rámci BCMS.
Zlepšenie procesov riadenia rizík a plánovania kontinuity: Audit podporuje systematický prístup k identifikácii, analýze a riadeniu rizík, ako aj k tvorbe a aktualizácii plánov kontinuity.
Zvýšenie efektivity a hospodárnosti BCMS: Implementácia odporúčaní z auditu môže priniesť optimalizáciu procesov BCMS a zníženie nákladov na riadenie kontinuity.
Posilnenie dôvery partnerov a investorov: Certifikácia ISO 22301 preukazuje záväzok k kontinuite prevádzky a posilňuje dôveru partnerov a investorov v odolnosť organizácie.

VYKONANIE AUDITU ALEBO GAP ANALÝZY PODĽA POŽIADAVIEK (SYSTÉM RIADENIA ICT SLUŽIEB) ISO 20000:1

Čo je?

Výkon auditu ISO 20000 je komplexný proces posudzovania súladu systému riadenia služieb IT (ITSM) organizácie s požiadavkami medzinárodnej normy ISO 20000. Audit zahŕňa:
Analýzu rizík: Identifikácia a hodnotenie rôznych typov rizík súvisiacich s poskytovaním IT služieb.
Posúdenie ITSM: Hodnotenie existujúcich procesov a opatrení ITSM a ich súladu s požiadavkami ISO 20000.
Testovanie kontrol: Testovanie vybraných kontrolných mechanizmov ITSM s cieľom overiť ich efektivitu.
Vypracovanie správy: Zhrnutie zistení auditu a odporúčaní na zlepšenie ITSM.

Prečo?

Zavedenie auditu ISO 20000 prináša viacero benefitov:
Zvýšenie súladu: Zabezpečenie súladu s požiadavkami ISO 20000, čím sa posilňuje dôvera partnerov a zákazníkov v kvalitu IT služieb. Zníženie rizík: Zvýšenie kvality a efektivity IT služieb a zníženie rizík súvisiacich s ich výpadkami alebo nesprávnym fungovaním. Zlepšenie procesov a opatrení: Implementácia odporúčaní z auditu môže optimalizovať procesy ITSM a zlepšiť celkovú kvalitu IT služieb. Zvýšenie konkurencieschopnosti: Dobre chránený informačný systém a certifikácia ISO 20000 môže priniesť organizácii konkurenčnú výhodu.

Pre koho?

Audit ISO 20000 je určený pre:

Organizácie, ktoré chcú preukázať záväzok ku kvalite IT služieb: Certifikácia ISO 20000 je medzinárodne uznávaným dôkazom o kvalite ITSM. Organizácie, ktoré chcú zlepšiť kvalitu a efektivitu IT služieb: Audit môže identifikovať oblasti, v ktorých je možné zlepšiť ITSM a znížiť riziká. Organizácie, ktoré sa chystajú na certifikáciu ISO 20000: Audit môže pomôcť organizácii pripraviť sa na certifikačný proces.

Prínosy?

Implementácia auditu ISO 20000 prináša nasledovné prínosy:

Zvýšenie povedomia o dôležitosti riadenia IT služieb: Audit zvyšuje povedomie manažmentu a zamestnancov o dôležitosti ITSM a ich zodpovednosti v rámci systému.
Zlepšenie procesov riadenia rizík a plánovania: Audit podporuje systematický prístup k identifikácii, analýze a riadeniu rizík súvisiacich s IT službami.
Zvýšenie efektivity a hospodárnosti ITSM: Implementácia odporúčaní z auditu môže priniesť optimalizáciu procesov ITSM a zníženie nákladov na IT služby.
Posilnenie dôvery partnerov a zákazníkov: Certifikácia ISO 20000 preukazuje záväzok k riadeniu a kvalite IT služieb a posilňuje dôveru partnerov a zákazníkov v organizáciu.

VYKONANIE AUDITU ALEBO GAP ANALÝZY PODĽA POŽIADAVIEK (PRIEMYSELNÁ BEZPEČNOSŤ)

Čo je?

Výkon auditu IEC 62443 je komplexný proces posudzovania súladu systému riadenia kybernetickej bezpečnosti (ISMS) organizácie s požiadavkami medzinárodnej normy IEC 62443. Audit zahŕňa:
Analýzu rizík: Identifikácia a hodnotenie rôznych typov kybernetických hrozieb a zraniteľností v súlade s definíciou IEC 62443. Posúdenie ISMS: Hodnotenie existujúcich procesov a opatrení ISMS a ich súladu s požiadavkami IEC 62443. Testovanie kontrol: Testovanie vybraných kontrolných mechanizmov ISMS s cieľom overiť ich efektivitu. Vypracovanie správy: Zhrnutie zistení auditu a odporúčaní na zlepšenie.

Prečo?

Zavedenie auditu IEC 62443 prináša viacero benefitov:
Zvýšenie súladu: Zabezpečenie súladu s požiadavkami IEC 62443, čím sa posilňuje dôvera partnerov a zákazníkov v kybernetickú odolnosť organizácie. Zníženie rizík: Zvýšenie kybernetickej odolnosti a zníženie rizika kybernetických incidentov. Zlepšenie procesov a opatrení: Implementácia odporúčaní z auditu môže optimalizovať procesy ISMS a zlepšiť celkovú kybernetickú odolnosť. Zvýšenie konkurencieschopnosti: Dobre chránený informačný systém a certifikácia IEC 62443 môže priniesť organizácii konkurenčnú výhodu.

Pre koho?

Audit IEC 62443 je určený pre:
Organizácie v prevádzkovateľoch kritickej infraštruktúry: Energetické siete, doprava, telekomunikácie a iné sektory definované v IEC 62443. Výrobcov automatizačných a riadiacich systémov: Dodávatelia komponentov a systémov pre kritickú infraštruktúru. Organizácie, ktoré chcú preukázať záväzok k kybernetickej bezpečnosti: Certifikácia IEC 62443 je medzinárodne uznávaným dôkazom o kvalite ISMS v oblasti kritickej infraštruktúry. Organizácie, ktoré sa chystajú na certifikáciu IEC 62443: Audit môže pomôcť organizácii pripraviť sa na certifikačný proces.

Prínosy?

Implementácia auditu IEC 62443 prináša nasledovné prínosy:
Zvýšenie povedomia o kybernetických hrozbách a rizikách: Audit zvyšuje povedomie manažmentu a zamestnancov o špecifických hrozbách a rizikách v oblasti kritickej infraštruktúry a ich zodpovednosti v rámci ISMS. Zlepšenie procesov riadenia rizík a kybernetickej odolnosti: Audit podporuje systematický prístup k identifikácii, analýze a riadeniu kybernetických rizík v súlade s požiadavkami IEC 62443.
Zníženie rizika kybernetických incidentov a dopadov na prevádzku: Včasná identifikácia a náprava zraniteľností a slabín v kybernetickej odolnosti znižuje riziko a dopady incidentov na prevádzku kritickej infraštruktúry. Posilnenie dôvery partnerov a zákazníkov: Certifikácia IEC 62443 preukazuje záväzok k kybernetickej bezpečnosti a odolnosti v kritickej infraštruktúre a posilňuje dôveru partnerov a zákazníkov v organizáciu.

VYKONANIE AUDITU ALEBO GAP ANALÝZY PODĽA POŽIADAVIEK (SYSTÉM RIADENIA KVALITY)

Čo je?

Výkon auditu ISO 9001 je komplexný proces posudzovania súladu systému manažérstva kvality (SMK) organizácie s požiadavkami medzinárodnej normy ISO 9001. Audit zahŕňa:
Analýzu rizík: Identifikácia a hodnotenie rôznych typov rizík ovplyvňujúcich kvalitu produktov a služieb v súlade s definíciou ISO 9001. Posúdenie SMK: Hodnotenie existujúcich procesov a opatrení SMK a ich súladu s požiadavkami ISO 9001. Testovanie kontrol: Testovanie vybraných kontrolných mechanizmov SMK s cieľom overiť ich efektivitu. Vypracovanie správy: Zhrnutie zistení auditu a odporúčaní na zlepšenie SMK.

Prečo?

Zavedenie auditu ISO 9001 prináša viacero benefitov:
Zvýšenie súladu: Zabezpečenie súladu s požiadavkami ISO 9001, čím sa posilňuje dôvera partnerov a zákazníkov v kvalitu produktov a služieb.
Zníženie rizík: Zvýšenie efektivity a zníženie rizík ovplyvňujúcich kvalitu produktov a služieb.
Zlepšenie procesov a opatrení: Implementácia odporúčaní z auditu môže optimalizovať procesy SMK a zlepšiť celkovú kvalitu produktov a služieb.
Zvýšenie konkurencieschopnosti: Dobre fungujúci systém manažérstva kvality a certifikácia ISO 9001 môže priniesť organizácii konkurenčnú výhodu.

Pre koho?

Audit ISO 9001 je určený pre:
Organizácie, ktoré chcú preukázať záväzok ku kvalite: Certifikácia ISO 9001 je medzinárodne uznávaným dôkazom o kvalite SMK. Organizácie, ktoré chcú zlepšiť kvalitu produktov a služieb: Audit môže identifikovať oblasti, v ktorých je možné zlepšiť SMK a znížiť riziká. Organizácie, ktoré sa chystajú na certifikáciu ISO 9001: Audit môže pomôcť organizácii pripraviť sa na certifikačný proces.

Prínosy?

Implementácia auditu ISO 9001 prináša nasledovné prínosy:

Zvýšenie povedomia o dôležitosti kvality: Audit zvyšuje povedomie manažmentu a zamestnancov o dôležitosti kvality a ich zodpovednosti v rámci SMK.
Zlepšenie procesov riadenia rizík a plánovania: Audit podporuje systematický prístup k identifikácii, analýze a riadeniu rizík ovplyvňujúcich kvalitu.
Zvýšenie efektivity a hospodárnosti SMK: Implementácia odporúčaní z auditu môže priniesť optimalizáciu procesov SMK a zníženie nákladov na riadenie kvality.
Posilnenie dôvery partnerov a zákazníkov: Certifikácia ISO 9001 preukazuje záväzok ku kvalitnému riadeniu.

VYKONANIE AUDITU ALEBO GAP ANALÝZY PODĽA POŽIADAVIEK REGULÁCIE GDPR O OCHRANE OSOBNÝCH ÚDAJOV

Čo je?

Výkon auditu GDPR (General Data Protection Regulation) je komplexný proces posudzovania súladu spracovania osobných údajov v organizácii s požiadavkami GDPR. Audit zahŕňa:
Analýzu rizík: Identifikácia a hodnotenie rôznych typov rizík súvisiacich s ochranou osobných údajov. Posúdenie súladu: Hodnotenie existujúcich procesov a opatrení na ochranu osobných údajov a ich súladu s GDPR. Testovanie kontrol: Testovanie vybraných kontrolných mechanizmov na ochranu osobných údajov s cieľom overiť ich efektivitu.

Prečo?

Zavedenie auditu GDPR prináša viacero benefitov:
Zvýšenie súladu: Zabezpečenie súladu s GDPR a minimalizácia rizika pokút a sankcií.
Zníženie rizík: Zvýšenie ochrany osobných údajov a zníženie rizika úniku alebo zneužitia týchto údajov.
Zlepšenie procesov a opatrení: Implementácia odporúčaní z auditu môže optimalizovať procesy ochrany osobných údajov a zlepšiť celkovú úroveň ochrany. Zvýšenie dôvery partnerov a zákazníkov: Preukázanie záväzku k ochrane osobných údajov posilňuje dôveru partnerov a zákazníkov v organizáciu.

Pre koho?

Audit GDPR je určený pre:

Organizácie, ktoré chcú preukázať záväzok k ochrane osobných údajov: Implementácia GDPR a audit sú dôležitými krokmi pre budovanie dôvery a transparentnosti v oblasti ochrany súkromia.
Organizácie, ktoré chcú zlepšiť ochranu osobných údajov: Audit môže identifikovať oblasti, v ktorých je možné zlepšiť procesy a opatrenia na ochranu osobných údajov. Organizácie, ktoré sa chystajú na certifikáciu GDPR: Audit môže pomôcť organizácii pripraviť sa na certifikačný proces.

Prínosy?

Implementácia auditu GDPR prináša nasledovné prínosy:
Zvýšenie povedomia o ochrane osobných údajov: Audit zvyšuje povedomie manažmentu a zamestnancov o dôležitosti ochrany osobných údajov a ich zodpovednosti v rámci GDPR. Zlepšenie procesov riadenia rizík a plánovania: Audit podporuje systematický prístup k identifikácii, analýze a riadeniu rizík súvisiacich s ochranou osobných údajov. Zníženie nákladov na sankcie a nápravu: Včasná identifikácia a náprava nedostatkov v ochrane osobných údajov znižuje riziko pokút a sankcií. Posilnenie dôvery partnerov a zákazníkov: Preukázanie záväzku k ochrane osobných údajov a súladu s GDPR posilňuje dôveru partnerov a zákazníkov v organizáciu.

VYKONANIE AUDITU ALEBO GAP ANALÝZY PODĽA POŽIADAVIEK AUTOMOTIVE ŠTANDARDU TISAX® VER.06

Čo je?

Výkon auditu TISAX® (Trusted Information Security Assessment Exchange) je komplexný proces posudzovania súladu informačnej bezpečnosti v automobilovom priemysle s požiadavkami medzinárodného štandardu TISAX®. Audit zahŕňa: Analýzu rizík: Identifikácia a hodnotenie rôznych typov rizík informačnej bezpečnosti relevantných pre automobilový priemysel. Posúdenie ISMS: Hodnotenie existujúcich procesov a opatrení informačnej bezpečnosti a ich súladu s požiadavkami TISAX®. Testovanie kontrol: Testovanie vybraných kontrolných mechanizmov informačnej bezpečnosti s cieľom overiť ich efektivitu. Vypracovanie správy: Zhrnutie zistení auditu a odporúčaní na zlepšenie informačnej bezpečnosti.

Prečo?

Zavedenie auditu TISAX® prináša viacero benefitov:
Zvýšenie súladu: Zabezpečenie súladu s požiadavkami TISAX® a posilnenie dôvery partnerov a zákazníkov v informačnú bezpečnosť dodávateľov v automobilovom priemysle. Zníženie rizík: Zvýšenie informačnej bezpečnosti a zníženie rizika kybernetických incidentov a narušenia dodávateľského reťazca. Zlepšenie procesov a opatrení: Implementácia odporúčaní z auditu môže optimalizovať procesy informačnej bezpečnosti a zlepšiť celkovú úroveň ochrany informácií. Zvýšenie konkurencieschopnosti: Preukázanie záväzku k informačnej bezpečnosti a certifikácia TISAX® môže priniesť dodávateľom v automobilovom priemysle konkurenčnú výhodu.

Pre koho?

Audit TISAX® je určený pre:
Dodávateľov v automobilovom priemysle: Výrobcovia automobilov a ich subdodávatelia, ktorí chcú preukázať súlad s požiadavkami TISAX® a posilniť dôveru v ich informačnú bezpečnosť. Organizácie, ktoré chcú zlepšiť informačnú bezpečnosť: Audit môže identifikovať oblasti, v ktorých je možné zlepšiť procesy a opatrenia informačnej bezpečnosti v súlade s požiadavkami relevantnými pre automobilový priemysel. Organizácie, ktoré sa chystajú na certifikáciu TISAX®: Audit môže pomôcť organizácii pripraviť sa na certifikačný proces.

Prínosy?

Implementácia auditu TISAX® prináša nasledovné prínosy:
Zvýšenie povedomia o informačnej bezpečnosti: Audit zvyšuje povedomie manažmentu a zamestnancov o dôležitosti informačnej bezpečnosti a ich zodpovednosti v rámci TISAX®. Zlepšenie procesov riadenia rizík a plánovania: Audit podporuje systematický prístup k identifikácii, analýze a riadeniu rizík informačnej bezpečnosti relevantných pre automobilový priemysel. Zníženie nákladov na kybernetické incidenty a narušenie dodávateľského reťazca: Včasná identifikácia a náprava nedostatkov v informačnej bezpečnosti znižuje riziko a dopady incidentov.
Posilnenie dôvery partnerov a zákazníkov: Preukázanie záväzku k informačnej bezpečnosti a certifikácia TISAX® posilňuje dôveru partnerov a zákazníkov v dodávateľov v automobilovom priemysle.

PORADENSTVO A POSKYTOVANIE SLUŽIEB V OBLASTI CLOUDOVÝCH SLUŽIEB ZAMERANÝCH NA BEZPEČNOSŤ PODĽA ISO 27017 A ISO 20018

Čo je?

Výkon auditu Cloudové služby je komplexný proces posudzovania súladu a bezpečnosti cloudového prostredia organizácie s požiadavkami relevantných noriem a osvedčených postupov. Audit zahŕňa: Analýzu rizík: Identifikácia a hodnotenie rôznych typov rizík súvisiacich s používaním cloudových služieb. Posúdenie cloudového prostredia: Hodnotenie existujúcich procesov a opatrení v cloudovom prostredí a ich súladu s požiadavkami na bezpečnosť a ochranu dát. Testovanie kontrol: Testovanie vybraných kontrolných mechanizmov v cloudovom prostredí s cieľom overiť ich efektivitu.

Prečo?

Zavedenie auditu Cloudové služby prináša viacero benefitov:
Zvýšenie súladu: Zabezpečenie súladu s relevantnými normami a regulačnými požiadavkami týkajúcimi sa cloudových služieb. Zníženie rizík: Zvýšenie bezpečnosti cloudového prostredia a zníženie rizika kybernetických incidentov a úniku dát. Zlepšenie procesov a opatrení: Implementácia odporúčaní z auditu môže optimalizovať procesy a posilniť ochranu dát v cloudovom prostredí. Posilnenie dôvery partnerov a zákazníkov: Preukázanie záväzku k bezpečnosti a súladu v cloude posilňuje dôveru partnerov a zákazníkov v organizáciu.

Pre koho?

Audit Cloudové služby je určený pre:
Organizácie, ktoré používajú cloudové služby: Všetky typy organizácií, ktoré využívajú cloudové služby pre rôzne účely, od uloženia dát až po spracovanie aplikácií. Organizácie, ktoré sa chystajú migrovať do cloudu: Audit môže pomôcť s posúdením pripravenosti na migráciu a identifikáciou potenciálnych rizík. Organizácie, ktoré chcú preukázať záväzok k bezpečnosti a súladu v cloude: Certifikácia na základe auditu môže posilniť dôveru partnerov a zákazníkov.

Prínosy?

Implementácia auditu Cloudové služby prináša nasledovné prínosy:

Zvýšenie povedomia o rizikách a požiadavkach na bezpečnosť v cloude: Audit zvyšuje povedomie manažmentu a zamestnancov o dôležitosti bezpečnosti a súladu v cloudovom prostredí.
Zlepšenie procesov riadenia rizík a plánovania: Audit podporuje systematický prístup k identifikácii, analýze a riadeniu rizík súvisiacich s cloudom. Zníženie nákladov na kybernetické incidenty a nápravu: Včasná identifikácia a náprava nedostatkov v cloudovej bezpečnosti znižuje riziko a dopady incidentov.
Posilnenie dôvery partnerov a zákazníkov: Preukázanie záväzku k bezpečnosti a súladu v cloude posilňuje dôveru partnerov a zákazníkov v organizáciu.

VYKONANIE AUDITU ALEBO GAP ANALÝZY PODĽA POŽIADAVIEK ŠTANDARDU OWASP, ASVS REL. 4.4 (5)

Čo je?

Výkon auditu Aplikačný audit podľa ISVS OWASP je komplexný proces posudzovania bezpečnosti webových aplikácií a webových služieb organizácie v súlade s požiadavkami Open Web Application Security Project (OWASP) Information Security Verification Standard (ISVS). Audit zahŕňa:
Analýzu rizík: Identifikácia a hodnotenie rôznych typov bezpečnostných rizík relevantných pre webové aplikácie a webové služby. Posúdenie aplikácie: Hodnotenie existujúcich bezpečnostných opatrení v aplikácii a ich súladu s požiadavkami ISVS OWASP. Testovanie penetrácie: Simulácia útokov na webovú aplikáciu a webové služby s cieľom overiť ich odolnosť voči známym zraniteľnostiam. Vypracovanie správy: Zhrnutie zistení auditu a odporúčaní na zlepšenie bezpečnosti webovej aplikácie a webových služieb.

Prečo?

Zavedenie auditu Aplikačný audit podľa ISVS OWASP prináša viacero benefitov:
Zvýšenie bezpečnosti: Zvýšenie odolnosti webovej aplikácie a webových služieb voči kybernetickým útokom a zraniteľnostiam. Zníženie rizík: Zníženie rizika úniku dát, narušenia prevádzky a reputácie v dôsledku bezpečnostných incidentov. Zlepšenie procesov a opatrení: Implementácia odporúčaní z auditu môže optimalizovať bezpečnostné procesy a posilniť ochranu webovej aplikácie a webových služieb.
Posilnenie dôvery partnerov a zákazníkov: Preukázanie záväzku k bezpečnosti webovej aplikácie a webových služieb posilňuje dôveru partnerov a zákazníkov v organizáciu.

Pre koho?

Audit Aplikačný audit podľa ISVS OWASP je určený pre:
Organizácie, ktoré prevádzkujú webové aplikácie a webové služby: Všetky typy organizácií, ktoré disponujú webovými aplikáciami a webovými službami, od jednoduchých webových stránok až po komplexné e-commerce platformy. Organizácie, ktoré sa chystajú spustiť novú webovú aplikáciu: Audit môže pomôcť s posúdením bezpečnosti aplikácie pred jej spustením a identifikáciou potenciálnych rizík. Organizácie, ktoré chcú preukázať záväzok k bezpečnosti webových aplikácií: Certifikácia na základe auditu môže posilniť dôveru partnerov a zákazníkov v organizáciu.

Prínosy?

Implementácia auditu Aplikačný audit podľa ISVS OWASP prináša nasledovné prínosy:
Zvýšenie povedomia o bezpečnostných rizikách webových aplikácií: Audit zvyšuje povedomie manažmentu a vývojárov o dôležitosti bezpečnosti webových aplikácií a webových služieb. Zlepšenie procesov riadenia rizík a plánovania: Audit podporuje systematický prístup k identifikácii, analýze a riadeniu bezpečnostných rizík webových aplikácií. Zníženie nákladov na nápravu bezpečnostných incidentov: Včasná identifikácia a náprava bezpečnostných zraniteľností v webovej aplikácii a webových službách znižuje riziko a dopady incidentov. Posilnenie dôvery partnerov a zákazníkov: Preukázanie záväzku k bezpečnosti webových aplikácií a webových služieb posilňuje dôveru partnerov a zákazníkov v organizáciu.

NAKIB

E-LEARNINGOVÉ SLUŽBY

NAKIB.SK

EFEKTÍVNE VZDELÁVANIE FORMOU E-LEARNINGOVEJ SLUŽBY

Čo je?

E-learningový softvér Základy informačnej bezpečnosti je online kurz, ktorý sa zameriava na edukáciu o základných princípoch informačnej bezpečnosti. Kurz môže obsahovať rôzne témy, ako napríklad: Identifikácia a hodnotenie rizík: Naučíte sa, ako identifikovať a hodnotiť rôzne typy informačných bezpečnostných rizík. Ochrana dát: Naučíte sa, ako chrániť citlivé dáta pred neoprávneným prístupom, použitím, zverejnením, zmenou alebo zničením. Riadenie prístupov: Naučíte sa, ako definovať a implementovať politiky riadenia prístupov k informáciám a systémom. Bezpečnosť sietí a zariadení: Naučíte sa, ako chrániť počítačové siete a zariadenia pred kybernetickými útokmi. Zálohovanie a obnova dát: Naučíte sa, ako zálohovať a obnovovať dáta v prípade incidentu informačnej bezpečnosti. Zákony a regulácie: Naučíte sa o relevantných zákonoch a reguláciách týkajúcich sa informačnej bezpečnosti.

Prečo?

Zavedenie e-learningového softvéru Základy informačnej bezpečnosti prináša viacero benefitov: Zvýšenie povedomia: Zvýšenie povedomia o informačnej bezpečnosti medzi zamestnancami a zníženie rizika kybernetických incidentov.Zníženie rizík: Zvýšenie informovanosti o rôznych typoch informačných bezpečnostných rizík a naučenie sa, ako ich predchádzať a riešiť. Zlepšenie súladu: Zabezpečenie súladu s relevantnými zákonmi a reguláciami týkajúcimi sa informačnej bezpečnosti. Zníženie nákladov: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadu môže priniesť značné úspory nákladov. Zvýšenie produktivity: Zvýšenie produktivity zamestnancov znížením prestojov súvisiacich s kybernetickými incidentmi.

Pre koho?

E-learningový softvér Základy informačnej bezpečnosti je určený pre:
Zamestnancov: Všetci zamestnanci by mali mať základné znalosti o informačnej bezpečnosti, aby sa vedeli chrániť pred kybernetickými hrozbami. Manažérov: Manažéri musia mať hlbšie znalosti o informačnej bezpečnosti, aby mohli efektívne riadiť riziká a chrániť firemné dáta. Študentov: Študenti, ktorí sa chcú venovať kariére v oblasti informačnej bezpečnosti, si v tomto kurze môžu vybudovať základné znalosti. Každý, kto sa chce dozvedieť viac o informačnej bezpečnosti.

Prínosy?

Implementácia e-learningového softvéru Základy informačnej bezpečnosti prináša nasledovné prínosy: Zvýšenie povedomia o informačnej bezpečnosti: Softvér umožňuje komplexnú edukáciu o rôznych aspektoch informačnej bezpečnosti a zvyšuje povedomie o kybernetických hrozbách. Zjednodušenie riadenia informačnej bezpečnosti: Softvér uľahčuje implementáciu a udržiavanie politík a procesov informačnej bezpečnosti. Zníženie rizík: Zvýšenie znalostí a zručností v oblasti informačnej bezpečnosti môže znížiť riziko kybernetických incidentov. Zlepšenie reputácie: Preukázanie záväzku k informačnej bezpečnosti posilňuje dôveru partnerov a zákazníkov. Zvýšenie konkurencieschopnosti: Dobre informovaní a edukovaní zamestnanci v oblasti informačnej bezpečnosti sú cenným prínosom pre každú firmu.

EFEKTÍVNE VZDELÁVANIE FORMOU E-LEARNINGOVEJ SLUŽBY

Čo je?

E-learningový softvér Základy kybernetickej bezpečnosti je online kurz, ktorý sa zameriava na edukáciu o základných princípoch kybernetickej bezpečnosti. Kurz môže obsahovať rôzne témy, ako napríklad:
Typy kybernetických hrozieb: Naučíte sa o rôznych typoch kybernetických hrozieb, ako sú malware, phishing, DDoS útoky a sociálne inžinierstvo. Ochrana zariadení: Naučíte sa, ako chrániť počítače, smartfóny a iné zariadenia pred kybernetickými útokmi. Bezpečnosť sietí: Naučíte sa, ako chrániť počítačové siete pred neoprávneným prístupom a útokmi. Bezpečnostné správanie: Naučíte sa o dôležitých bezpečnostných návykoch, ako je silné heslo a obozretnosť pri používaní online služieb. Zákon a regulácie: Naučíte sa o relevantných zákonoch a reguláciách týkajúcich sa kybernetickej bezpečnosti.

Prečo?

Zavedenie e-learningového softvéru Základy kybernetickej bezpečnosti prináša viacero benefitov:
Zvýšenie povedomia: Zvýšenie povedomia o kybernetických hrozbách medzi zamestnancami a zníženie rizika kybernetických incidentov. Zníženie rizík: Zvýšenie informovanosti o rôznych typoch kybernetických hrozieb a naučenie sa, ako ich predchádzať a riešiť. Zlepšenie súladu: Zabezpečenie súladu s relevantnými zákonmi a reguláciami týkajúcimi sa kybernetickej bezpečnosti. Zníženie nákladov: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadu môže priniesť značné úspory nákladov. Zvýšenie produktivity: Zvýšenie produktivity zamestnancov znížením prestojov súvisiacich s kybernetickými incidentmi.

Pre koho?

E-learningový softvér Základy kybernetickej bezpečnosti je určený pre:
Zamestnancov: Všetci zamestnanci by mali mať základné znalosti o kybernetickej bezpečnosti, aby sa vedeli chrániť pred kybernetickými hrozbami. Manažérov: Manažéri musia mať hlbšie znalosti o kybernetickej bezpečnosti, aby mohli efektívne riadiť riziká a chrániť firemné dáta. Študentov: Študenti, ktorí sa chcú venovať kariére v oblasti kybernetickej bezpečnosti, si v tomto kurze môžu vybudovať základné znalosti. Každý, kto sa chce dozvedieť viac o kybernetickej bezpečnosti.

Prínosy?

Implementácia e-learningového softvéru Základy kybernetickej bezpečnosti prináša nasledovné prínosy:
Zvýšenie povedomia o kybernetickej bezpečnosti: Softvér umožňuje komplexnú edukáciu o rôznych aspektoch kybernetickej bezpečnosti a zvyšuje povedomie o kybernetických hrozbách. Zjednodušenie riadenia kybernetickej bezpečnosti: Softvér uľahčuje implementáciu a udržiavanie politík a procesov kybernetickej bezpečnosti. Zníženie rizík: Zvýšenie znalostí a zručností v oblasti kybernetickej bezpečnosti môže znížiť riziko kybernetických incidentov. Zlepšenie reputácie: Preukázanie záväzku k kybernetickej bezpečnosti posilňuje dôveru partnerov a zákazníkov. Zvýšenie konkurencieschopnosti: Dobre informovaní a edukovaní zamestnanci v oblasti kybernetickej bezpečnosti sú cenným prínosom pre každú firmu.

EFEKTÍVNE VZDELÁVANIE FORMOU E-LEARNINGOVEJ SLUŽBY

Čo je?

E-learningový softvér Základy ochrany osobných údajov je online kurz, ktorý sa zameriava na edukáciu o základných princípoch ochrany osobných údajov v súlade s GDPR (General Data Protection Regulation). Kurz môže obsahovať rôzne témy, ako napríklad: Definícia a typy osobných údajov: Naučíte sa, aké informácie sa považujú za osobné údaje a aké sú rôzne typy osobných údajov. Princípy ochrany osobných údajov: Naučíte sa o základných princípoch ochrany osobných údajov, ako je zákonnosť, spravodlivosť a transparentnosť. Práva dotknutých osôb: Naučíte sa o právach dotknutých osôb, ako je právo na prístup k informáciám, právo na opravu a právo na výmaz. Povinnosti prevádzkovateľov a sprostredkovateľov: Naučíte sa o povinnostiach prevádzkovateľov a sprostredkovateľov osobných údajov, ako je vedenie záznamov o spracovateľských aktivitách a implementácia technických a organizačných opatrení na ochranu osobných údajov.
Sankcie za porušenie GDPR: Naučíte sa o sankciách za porušenie GDPR.

Prečo?

Zavedenie e-learningového softvéru Základy ochrany osobných údajov prináša viacero benefitov:
Zvýšenie povedomia: Zvýšenie povedomia o GDPR a ochrane osobných údajov medzi zamestnancami a zníženie rizika porušenia GDPR. Zníženie rizík: Zvýšenie informovanosti o rôznych aspektoch ochrany osobných údajov a naučenie sa, ako dodržiavať GDPR. Zlepšenie súladu: Zabezpečenie súladu s GDPR a minimalizácia rizika sankcií. Zníženie nákladov: Predchádzanie porušeniam GDPR a minimalizácia ich dopadu môže priniesť značné úspory nákladov. Zvýšenie reputácie: Preukázanie záväzku k ochrane osobných údajov posilňuje dôveru partnerov a zákazníkov.

Pre koho?

E-learningový softvér Základy ochrany osobných údajov je určený pre:
Zamestnancov: Všetci zamestnanci by mali mať základné znalosti o GDPR a ochrane osobných údajov, aby sa vedeli správať zodpovedne s citlivými informáciami. Manažérov: Manažéri musia mať hlbšie znalosti o GDPR a ochrane osobných údajov, aby mohli efektívne riadiť riziká a chrániť firemné dáta. Študentov: Študenti, ktorí sa chcú venovať kariére v oblasti ochrany osobných údajov, si v tomto kurze môžu vybudovať základné znalosti. Každý, kto sa chce dozvedieť viac o GDPR a ochrane osobných údajov.

Prínosy?

Implementácia e-learningového softvéru Základy ochrany osobných údajov prináša nasledovné prínosy:
Zvýšenie povedomia o GDPR a ochrane osobných údajov: Softvér umožňuje komplexnú edukáciu o rôznych aspektoch GDPR a ochrany osobných údajov a zvyšuje povedomie o relevantných pravidlách a povinnostiach. Zjednodušenie dodržiavania GDPR: Softvér uľahčuje implementáciu a udržiavanie politík a procesov potrebných pre súlad s GDPR. Zníženie rizík porušenia GDPR: Zvýšenie znalostí a zručností v oblasti ochrany osobných údajov môže znížiť riziko porušenia GDPR. Zlepšenie reputácie: Preukázanie záväzku k ochrane osobných údajov posilňuje dôveru partnerov a zákazníkov.Zvýšenie konkurencieschopnosti: Dobre informovaní a edukovaní zamestnanci.

EFEKTÍVNE VZDELÁVANIE FORMOU E-LEARNINGOVEJ SLUŽBY

Čo je?

E-learningový softvér Základy biznis kontinuity je online kurz, ktorý sa zameriava na edukáciu o základných princípoch riadenia kontinuity biznisu (BCMS). Kurz môže obsahovať rôzne témy, ako napríklad: Identifikácia a hodnotenie rizík: Naučíte sa, ako identifikovať a hodnotiť rôzne typy rizík, ktoré by mohli narušiť prevádzku organizácie. Plánovanie kontinuity: Naučíte sa, ako definovať plány kontinuity pre rôzne typy krízových scenárov. Implementácia a testovanie: Naučíte sa, ako implementovať a testovať plány kontinuity. Monitorovanie a reporting: Naučíte sa, ako monitorovať a reportovať o stave kontinuity biznisu.

Prečo?

Zavedenie e-learningového softvéru Základy biznis kontinuity 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?

E-learningový softvér Základy biznis kontinuity 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 e-learningového softvéru Základy biznis kontinuity 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 rôznych tímov v rámci krízovej situácie. Zvýšenie konkurencieschopnosti: Preukázanie záväzku k riadeniu kontinuity biznisu posilňuje dôveru partnerov a zákazníkov a môže zlepšiť konkurencieschopnosť na trhu.

EFEKTÍVNE VZDELÁVANIE DORA FORMOU E-LEARNINGOVEJ SLUŽBY

Čo je?

Regulácia DORA (Digital Operational Resilience Act) je komplexný proces posudzovania súladu informačného systému a kybernetickej odolnosti organizácie s požiadavkami nariadenia DORA. Audit zahŕňa:
Analýzu rizík: Identifikácia a hodnotenie rôznych typov rizík prevádzkových výpadkov a kybernetických hrozieb v súlade s definíciou DORA. Posúdenie riadenia kybernetickej odolnosti: Hodnotenie existujúcich procesov a opatrení riadenia kybernetickej odolnosti v organizácii a ich súladu s požiadavkami DORA. Testovanie odolnosti: Simulácia rôznych scenárov prevádzkových výpadkov a kybernetických útokov s cieľom otestovať odolnosť informačného systému a reakcie organizácie. Vypracovanie správy: Zhrnutie zistení auditu a odporúčaní na zlepšenie kybernetickej odolnosti v súlade s nariadením DORA.

Prečo?

Vzdelávanie štandardu DORA prináša viacero benefitov:
Zvýšenie súladu: Zabezpečenie súladu s požiadavkami nariadenia DORA, čím sa minimalizuje riziko sankcií a administratívnych pokút. Zníženie rizík: Zvýšenie kybernetickej odolnosti a zníženie rizika prevádzkových výpadkov a kybernetických incidentov. Zlepšenie kontinuity prevádzky: Implementácia odporúčaní z auditu môže posilniť kontinuitu prevádzky a minimalizovať dopady výpadkov a incidentov. Zvýšenie konkurencieschopnosti: Dobre chránený informačný systém a vysoká kybernetická odolnosť môže priniesť organizácii konkurenčnú výhodu.

Pre koho?

Vzdelávanie DORA je určený pre:
Finančné inštitúcie: Banky, poisťovne, investičné firmy a iné subjekty podliehajúce nariadeniu DORA. Poskytovateľov kritickej infraštruktúry: Prevádzkovatelia energetických sietí, telekomunikácií, dopravy a iných kritických sektorov definovaných v DORA.Organizácie, ktoré chcú zlepšiť kybernetickú odolnosť: Audit môže identifikovať oblasti, v ktorých je možné zlepšiť kybernetickú odolnosť a súlad s požiadavkami DORA. Organizácie, ktoré sa chystajú na certifikáciu kybernetickej odolnosti: Audit môže pomôcť organizácii pripraviť sa na certifikáciu podľa medzinárodných štandardov s ohľadom na špecifiká DORA.

Prínosy?

Vzdelávanie štandardu DORA prináša nasledovné prínosy:
Zvýšenie povedomia o rizikách prevádzkových výpadkov a kybernetických hrozieb: Audit sa zameriava na špecifické hrozby a riziká definované v DORA, čím zvyšuje povedomie manažmentu a zamestnancov v daných oblastiach. Zlepšenie procesov a opatrení riadenia kybernetickej odolnosti: Audit identifikuje oblasti, v ktorých je nutné implementovať alebo upraviť procesy a opatrenia riadenia kybernetickej odolnosti tak, aby spĺňali požiadavky DORA. Zníženie rizika prevádzkových výpadkov a kybernetických incidentov: Včasná identifikácia a náprava zraniteľností a slabín v kybernetickej odolnosti znižuje riziko a dopady výpadkov a incidentov.

EFEKTÍVNE VZDELÁVANIE ZÁKLADY TISAX® FORMOU E-LEARNINGOVEJ SLUŽBY

Čo je?

E-learningový softvér Základy TISAX je online kurz, ktorý sa zameriava na edukáciu o základných princípoch informačnej bezpečnosti v automobilovom priemysle podľa požiadaviek TISAX (Trusted Information Security Assessment Exchange). Kurz môže obsahovať rôzne témy, ako napríklad:
Základné pojmy TISAX: Naučíte sa o histórii a cieľoch TISAX, rôznych úrovniach auditu a relevantných dokumentoch. Požiadavky na informačnú bezpečnosť: Naučíte sa o požiadavkách TISAX na riadenie rizík, ochranu dát, riadenie prístupov, bezpečnosť sietí a zariadení, incident response a kontinuitu biznisu. Proces auditu TISAX: Naučíte sa o priebehu auditu TISAX, príprave na audit a nápravných opatreniach. Praktické tipy: Naučíte sa o praktických tipoch a nástrojoch na implementáciu požiadaviek TISAX.

Prečo?

Zavedenie e-learningového softvéru Základy TISAX prináša viacero benefitov:
Zvýšenie povedomia o TISAX: Zvýšenie povedomia o požiadavkách TISAX medzi zamestnancami a dodávateľmi v automobilovom priemysle. Zlepšenie súladu: Zabezpečenie súladu s požiadavkami TISAX a zníženie rizika neúspešného auditu. Zníženie rizík: Zvýšenie informačnej bezpečnosti a zníženie rizika kybernetických incidentov. Zlepšenie reputácie: Preukázanie záväzku k informačnej bezpečnosti posilňuje dôveru partnerov a zákazníkov. Zvýšenie konkurencieschopnosti: Dodržiavanie požiadaviek TISAX môže zlepšiť konkurencieschopnosť na trhu automobilového priemyslu.

Pre koho?

E-learningový softvér Základy TISAX je určený pre:
Zamestnancov: Všetci zamestnanci v automobilovom priemysle by mali mať základné znalosti o TISAX a požiadavkách na informačnú bezpečnosť. Manažérov: Manažéri musia mať hlbšie znalosti o TISAX a požiadavkách na informačnú bezpečnosť, aby mohli efektívne riadiť riziká a chrániť firemné dáta.
Dodávateľov: Dodávatelia v automobilovom priemysle musia spĺňať požiadavky TISAX, aby mohli spolupracovať s výrobcami automobilov. Audítorov: Audítori TISAX musia mať hlboké znalosti o požiadavkách TISAX a procese auditu. Každý, kto sa chce dozvedieť viac o TISAX a informačnej bezpečnosti v automobilovom priemysle.

Prínosy?

Implementácia e-learningového softvéru Základy TISAX prináša nasledovné prínosy:
Zvýšenie povedomia o TISAX a požiadavkách na informačnú bezpečnosť: Softvér umožňuje komplexnú edukáciu o rôznych aspektoch TISAX a informačnej bezpečnosti v automobilovom priemysle. Zjednodušenie implementácie TISAX: Softvér uľahčuje implementáciu a udržiavanie požiadaviek TISAX. Zníženie rizík kybernetických incidentov: Zvýšenie znalostí a zručností v oblasti informačnej bezpečnosti môže znížiť riziko kybernetických incidentov. Zlepšenie reputácie: Preukázanie záväzku k informačnej bezpečnosti a súladu s TISAX posilňuje dôveru partnerov a zákazníkov. Zvýšenie konkurencieschopnosti: Dobre informovaní a edukovaní zamestnanci a dodávatelia v oblasti TISAX a informačnej bezpečnosti sú cenným prínosom pre každú firmu v automobilovom priemysle.

EFEKTÍVNE VZDELÁVANIE TISAX® POKROČILÍ FORMOU E-LEARNINGOVEJ SLUŽBY

Čo je?

E-learningový softvér TISAX Pokročilí - Ochrana prototypov a GDPR je online kurz, ktorý sa zameriava na komplexnú edukáciu o pokročilých témach informačnej bezpečnosti v automobilovom priemysle v súlade s požiadavkami TISAX a GDPR. Kurz sa zameriava na dve kľúčové oblasti: Ochrana prototypov:
Dôvernosť prototypov: Naučíte sa o rôznych typoch prototypov a o tom, ako ich chrániť pred neoprávneným prístupom, použitím a zverejnením. Riadenie prístupov: Naučíte sa o definovaní a implementácii politík riadenia prístupov k prototypom. Technické riešenia: Naučíte sa o rôznych technických riešeniach na ochranu prototypov, ako sú šifrovanie, pseudonymizácia a watermarking.
Požiadavky GDPR: Naučíte sa o požiadavkách GDPR na spracovanie osobných údajov v kontexte TISAX.
Práva dotknutých osôb: Naučíte sa o právach dotknutých osôb, ako je právo na prístup k informáciám a právo na výmaz. Implementácia GDPR: Naučíte sa o tom, ako implementovať GDPR v praxi v kontexte TISAX.

Prečo?

Zavedenie e-learningového softvéru TISAX Pokročilí - Ochrana prototypov a GDPR prináša viacero benefitov: Zvýšenie povedomia o pokročilých témach informačnej bezpečnosti: Zvýšenie povedomia o dôležitosti ochrany prototypov a súladu s GDPR. Zlepšenie súladu: Zabezpečenie súladu s požiadavkami TISAX a GDPR a zníženie rizika sankcií. Zníženie rizík: Zvýšenie informačnej bezpečnosti a zníženie rizika kybernetických incidentov. Zlepšenie reputácie: Preukázanie záväzku k informačnej bezpečnosti a súladu s GDPR posilňuje dôveru partnerov a zákazníkov. Zvýšenie konkurencieschopnosti: Dobre informovaní a edukovaní zamestnanci v oblasti ochrany prototypov a GDPR sú cenným prínosom pre každú firmu v automobilovom priemysle.

Pre koho?

E-learningový softvér TISAX Pokročilí - Ochrana prototypov a GDPR je určený pre:
Manažérov: Manažéri musia mať hlbšie znalosti o ochrane prototypov a GDPR, aby mohli efektívne riadiť riziká a chrániť firemné dáta. Vývojárov: Vývojári prototypov musia mať znalosti o tom, ako chrániť prototypy pred neoprávneným prístupom a zneužitím. IT profesionálov: IT profesionáli musia mať znalosti o implementácii technických riešení na ochranu prototypov a o súlade s GDPR. Audítorov: Audítori TISAX a GDPR musia mať hlboké znalosti o požiadavkách TISAX a GDPR a o procese auditu. Každý, kto sa chce dozvedieť viac o ochrane prototypov a GDPR v kontexte TISAX.

Prínosy?

Implementácia e-learningového softvéru TISAX Pokročilí - Ochrana prototypov a GDPR prináša nasledovné prínosy:
Zvýšenie povedomia o ochrane prototypov a GDPR: Softvér umožňuje komplexnú edukáciu o rôznych aspektoch ochrany prototypov a GDPR. Zjednodušenie implementácie TISAX a GDPR: Softvér uľahčuje implementáciu a udržiavanie požiadaviek TISAX a GDPR. Zníženie rizík kybernetických incidentov: Zvýšenie znalostí a zručností v oblasti informačnej bezpečnosti a GDPR môže znížiť riziko kybernetických incidentov.

NAKIB

OUTSOURCOVANÉ ROLE

NAKIB.SK

OUTSOURCING ROLE “MKB” (MANAŽÉR KYBERNETICKEJ BEZPEČNOSTI)

Čo je?

Outsourcing role Výkon MKB (Manažér Kybernetickej Bezpečnosti) je prenesenie zodpovednosti za riadenie kybernetickej bezpečnosti na externého poskytovateľa služieb. Poskytovateľ služieb MKB preberá zodpovednosť za: Vypracovanie a implementáciu stratégie kybernetickej bezpečnosti: Stratégia definuje ciele a postupy pre ochranu informačných aktív organizácie pred kybernetickými hrozbami. Riadenie a aktualizácia programov kybernetickej bezpečnosti: Pravidelná aktualizácia programov zaisťuje ich efektivitu v reálnych podmienkach.Implementácia a správa bezpečnostných technológií: Poskytovateľ MKB implementuje a spravuje nástroje a technológie na ochranu informačných aktív. Monitorovanie a analýza bezpečnostných incidentov: Poskytovateľ MKB monitoruje a analyzuje bezpečnostné incidenty a hrozby a navrhuje riešenia.
Vzdelávanie a zvyšovanie povedomia o kybernetickej bezpečnosti: Poskytovateľ MKB komunikuje s manažmentom a zamestnancami o kybernetickej bezpečnosti a ich úlohách v rámci ochrany informačných aktív.

Prečo?

Zavedenie outsourcingu role Výkon MKB (Manažér Kybernetickej Bezpečnosti) prináša viacero benefitov:
Zníženie nákladov: Outsourcing MKB môže byť nákladovo efektívnejší ako interné budovanie a udržiavanie tímu pre kybernetickú bezpečnosť. Získanie prístupu k expertom: Poskytovatelia MKB disponujú skúseným tímom expertov s rozsiahlymi znalosťami a osvedčenými postupmi v oblasti kybernetickej bezpečnosti.
Zvýšenie efektivity: Outsourcing MKB umožňuje organizácii sústrediť sa na svoje kľúčové aktivity a nechať riadenie kybernetickej bezpečnosti na expertov. Zlepšenie súladu: Poskytovatelia MKB sú neustále aktualizovaní o najnovších hrozbách a reguláciách v oblasti kybernetickej bezpečnosti, čím vám pomôžu udržať súlad.

Pre koho?

Outsourcing role Výkon MKB (Manažér Kybernetickej Bezpečnosti) je určený pre:
Organizácie, ktoré chcú zefektívniť riadenie kybernetickej bezpečnosti: Outsourcing MKB môže pomôcť znížiť náklady a zlepšiť efektivitu riadenia rizík. Organizácie, ktoré nemajú interné kapacity pre riadenie kybernetickej bezpečnosti: Outsourcing MKB umožňuje organizáciám s malým tímom alebo bez skúseností s kybernetickou bezpečnosťou riadiť ochranu informačných aktív efektívne. Organizácie, ktoré sa chcú sústrediť na svoje kľúčové aktivity: Outsourcing MKB umožňuje organizácii presunúť zodpovednosť za riadenie kybernetickej bezpečnosti na externého partnera a sústrediť sa na svoje core aktivity.

Prínosy?

Implementácia outsourcingu role Výkon MKB (Manažér Kybernetickej Bezpečnosti) prináša nasledovné prínosy:
Zvýšenie úrovne kybernetickej bezpečnosti: MKB zaisťuje ochranu informačných aktív organizácie pred kybernetickými hrozbami a incidentmi. Zníženie rizika reputácie a finančných strát: MKB pomáha predchádzať strate reputácie a finančným stratám v dôsledku kybernetických útokov. Zlepšenie morálky a produktivity zamestnancov: Jasná stratégia a efektívna reakcia na incidenty zvyšuje morálku a produktivitu zamestnancov. Posilnenie dôvery partnerov a zákazníkov: MKB posilňuje dôveru partnerov a zákazníkov.

OUTSOURCING ROLE "DPO", (DATA PRIVACY OFFICER) PODĽA POŽIADAVIEK REGULÁCIE GDPR

Čo je?

Outsourcing role Výkon DPO (Data Privacy Officer) je prenesenie zodpovednosti za plnenie úloh DPO (poverenca pre ochranu osobných údajov) na externého poskytovateľa služieb. Poskytovateľ služieb DPO preberá zodpovednosť za: Dodržiavanie GDPR a iných relevantných predpisov: Poskytovateľ DPO sa stará o to, aby organizácia plnila všetky požiadavky na ochranu osobných údajov. Poskytovanie poradenstva a usmernení: Poskytovateľ DPO radí organizácii v otázkach ochrany osobných údajov a navrhuje riešenia na splnenie požiadaviek GDPR. Spolupráca s dozorným orgánom: Poskytovateľ DPO komunikuje s dozorným orgánom v mene organizácie a zodpovedá za plnenie jeho požiadaviek. Dohľad nad spracovaním osobných údajov: Poskytovateľ DPO monitoruje spracovanie osobných údajov v organizácii a kontroluje súlad s GDPR.

Prečo?

Zavedenie outsourcingu role Výkon DPO prináša viacero benefitov:
Zníženie nákladov: Outsourcing DPO môže byť nákladovo efektívnejší ako interné zamestnávanie DPO.
Získanie prístupu k expertom: Poskytovatelia DPO disponujú skúseným tímom expertov s rozsiahlymi znalosťami a osvedčenými postupmi v oblasti ochrany osobných údajov. Zvýšenie efektivity: Outsourcing DPO umožňuje organizácii sústrediť sa na svoje kľúčové aktivity a nechať ochranu osobných údajov na expertov. Zlepšenie súladu: Poskytovatelia DPO sú neustále aktualizovaní o najnovších požiadavkách a reguláciách v oblasti GDPR, čím vám pomôžu udržať súlad.

Pre koho?

Outsourcing role Výkon DPO je určený pre:
Organizácie, ktoré chcú zefektívniť ochranu osobných údajov: Outsourcing DPO môže pomôcť znížiť náklady a zlepšiť efektivitu riadenia rizík. Organizácie, ktoré nemajú interné kapacity pre ochranu osobných údajov: Outsourcing DPO umožňuje organizáciám s malým tímom alebo bez skúseností s GDPR riadiť ochranu osobných údajov efektívne. Organizácie, ktoré sa chcú sústrediť na svoje kľúčové aktivity: Outsourcing DPO umožňuje organizácii presunúť zodpovednosť za ochranu osobných údajov na externého partnera a sústrediť sa na svoje core aktivity.

Prínosy?

Implementácia outsourcingu role Výkon DPO prináša nasledovné prínosy:
Zvýšenie úrovne ochrany osobných údajov: DPO zaisťuje, že organizácia spĺňa všetky požiadavky GDPR a chráni osobné údaje pred zneužitím.
Zníženie rizika sankcií: DPO pomáha predchádzať sankciám za porušenie GDPR.
Zlepšenie morálky a produktivity zamestnancov.

OUTSOURCING ROLE “IA”, (INTERNÝ AUDÍTOR) PRE MANAŽÉRSKE SYSTÉMY ISO 9001, ISO 27001, ISO 22301, TISAX, ETC...

Čo je?

Outsourcing role Výkon IA (Interný Auditor) je prenesenie zodpovednosti za interné audity na externého poskytovateľa služieb. Poskytovateľ IA preberá zodpovednosť za:
Plánovanie a realizácia interných auditov: Poskytovateľ IA definuje harmonogram auditov a vykonáva audity v súlade s normami a osvedčenými postupmi. Vypracovanie a prezentácia správy z auditu: Poskytovateľ IA analyzuje zistenia z auditu a prezentuje ich manažmentu s odporúčaniami na zlepšenie. Sledovanie a implementácia nápravných opatrení: Poskytovateľ IA monitoruje implementáciu nápravných opatrení navrhovaných v správe z auditu. Poradenstvo a usmernenia: Poskytovateľ IA radí manažmentu v otázkach riadenia rizík a interných kontrol.

Prečo?

Zavedenie outsourcingu role Výkon IA prináša viacero benefitov:
Zníženie nákladov: Outsourcing IA môže byť nákladovo efektívnejší ako interné zamestnávanie interných audítorov. Získanie prístupu k expertom: Poskytovatelia IA disponujú skúseným tímom expertov s rozsiahlymi znalosťami a osvedčenými postupmi v oblasti interných auditov.
Zvýšenie efektivity: Outsourcing IA umožňuje organizácii sústrediť sa na svoje kľúčové aktivity a nechať interné audity na expertov. Zlepšenie objektivity: Externí audítori prinášajú do procesu auditu nezávislý pohľad a objektivitu.

Pre koho?

Outsourcing role Výkon IA je určený pre:
Organizácie, ktoré chcú zefektívniť interné audity: Outsourcing IA môže pomôcť znížiť náklady a zlepšiť efektivitu riadenia rizík. Organizácie, ktoré nemajú interné kapacity pre interné audity: Outsourcing IA umožňuje organizáciám s malým tímom alebo bez skúseností s internými auditmi riadiť riziká efektívne.
Organizácie, ktoré sa chcú sústrediť na svoje kľúčové aktivity: Outsourcing IA umožňuje organizácii presunúť zodpovednosť za interné audity na externého partnera a sústrediť sa na svoje core aktivity.

Prínosy?

Implementácia outsourcingu role Výkon IA prináša nasledovné prínosy:
Zvýšenie úrovne riadenia rizík: Interné audity pomáhajú identifikovať a riešiť riziká v organizácii.
Zlepšenie súladu: Interné audity overujú súlad s normami a predpismi.
Zvýšenie efektivity procesov: Interné audity identifikujú príležitosti na zlepšenie procesov a ich efektivity.
Posilnenie dôvery partnerov a zákazníkov: Interné audity posilňujú dôveru partnerov a zákazníkov v transparentnosť a zodpovednosť organizácie.

OUTSOURCING ROLE "SLUŽIEB SOC", (SECURITY OPERATION CENTER) AKO POŽIADAVKA KYBER BEZPEČNOSTI

Čo je?

Outsourcing role Výkon SOC Služieb (Security Operation Center) je prenesenie zodpovednosti za prevádzku a monitorovanie SOC centra na externého poskytovateľa služieb. Poskytovateľ SOC preberá zodpovednosť za: Neustály monitoring a analýza bezpečnostných udalostí: Poskytovateľ SOC 24/7 monitoruje a analyzuje bezpečnostné incidenty v sieti a systémoch organizácie. Identifikácia a reakcia na hrozby: Poskytovateľ SOC identifikuje a reaguje na kybernetické hrozby v reálnom čase. Vyšetrovanie incidentov a forenzná analýza: Poskytovateľ SOC analyzuje incidenty a zbiera forenzné dôkazy pre hlbšie pochopenie a prevenciu budúcich hrozieb. Reporting a komunikácia: Poskytovateľ SOC informuje manažment o bezpečnostnej situácii a o riešených incidentoch.

Prečo?

Zavedenie outsourcingu role Výkon SOC Služieb prináša viacero benefitov:
Zníženie nákladov: Outsourcing SOC môže byť nákladovo efektívnejší ako interné budovanie a prevádzka SOC centra. Získanie prístupu k expertom: Poskytovatelia SOC disponujú skúseným tímom expertov s rozsiahlymi znalosťami a osvedčenými postupmi v oblasti kybernetickej bezpečnosti. Zvýšenie efektivity: Outsourcing SOC umožňuje organizácii sústrediť sa na svoje kľúčové aktivity a nechať monitorovanie a reakciu na hrozby na expertov. Zvýšenie úrovne kybernetickej bezpečnosti: SOC centrum s nepretržitým monitoringom a expertnou analýzou posilňuje ochranu organizácie pred kybernetickými hrozbami.

Pre koho?

Outsourcing role Výkon SOC Služieb je určený pre:
Organizácie, ktoré chcú zefektívniť kybernetickú bezpečnosť: Outsourcing SOC môže pomôcť znížiť náklady a zlepšiť efektivitu riadenia rizík. Organizácie, ktoré nemajú interné kapacity pre prevádzku SOC centra: Outsourcing SOC umožňuje organizáciám s malým tímom alebo bez skúseností s kybernetickou bezpečnosťou riadiť ochranu informačných aktív efektívne. Organizácie, ktoré sa chcú sústrediť na svoje kľúčové aktivity: Outsourcing SOC umožňuje organizácii presunúť zodpovednosť za prevádzku SOC centra na externého partnera a sústrediť sa na svoje core aktivity.

Prínosy?

Implementácia outsourcingu role Výkon SOC Služieb prináša nasledovné prínosy:
Zvýšenie úrovne kybernetickej bezpečnosti: SOC centrum s nepretržitým monitoringom a expertnou analýzou posilňuje ochranu organizácie pred kybernetickými hrozbami. Rýchla reakcia na incidenty: Poskytovateľ SOC dokáže rýchlo a efektívne reagovať na kybernetické incidenty a minimalizovať ich dopady. Zníženie rizika reputácie a finančných strát: SOC centrum pomáha predchádzať strate reputácie a finančným stratám v dôsledku kybernetických útokov. Zlepšenie morálky a produktivity zamestnancov: Vedomie o nepretržitej ochrane SOC centra zvyšuje morálku a produktivitu zamestnancov.

NAKIB

SOFTWAROVÉ VYBAVENIE

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.

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.

NAKIB

ŠKOLENIA PRE SOC SLUŽBY

NAKIB.SK

ŠKOLENIA NA PRÍPRAVU TECHNICKÝCH ŠPECIALISTOV A ODBORNÍKOV (SOC) NA KYBERNETICKÚ BEZPEČNOSŤ NA REÁLNE RIEŠENIA INCIDENTOV V ORGANIZÁCII

Čo je?

Vzdelávanie v oblasti Real World Penetration Testing je špecializovaný kurz zameraný na výcvik účastníkov v technikách a metódach používaných na identifikáciu a zneškodnenie zraniteľností v informačných systémoch a sieťových infraštruktúrach. Cieľom je naučiť účastníkov, ako realizovať simulované útoky na systémy s cieľom nájsť a opraviť bezpečnostné slabiny predtým, ako ich využijú skutoční útočníci.
Školenie je rozdelené na 4 časti (rovnako ako samotný proces riešenia incidentov):

- Príprava na riešenie bezpečnostného incidentu
- Detekcia a analýza kybernetického incidentu
- Obmedzenie šírenia bezpečnostného incidentu ,Eradication a Obnova
- Systémové zmeny v bezpečnostnom prostredí organizácie

Prečo?

Zvýšenie bezpečnostných zručností: Kurz poskytuje hlboké pochopenie bezpečnostných hrozieb, zraniteľností a techník ich odhaľovania a eliminácie. Účastníci sa naučia, ako identifikovať a opraviť slabiny, čím zlepšujú svoje schopnosti ochrany IT infraštruktúry. Prevencia bezpečnostných incidentov: V dnešnej dobe, keď sú kybernetické útoky čoraz sofistikovanejšie, je dôležité byť o krok vpred pred útočníkmi. Penetračné testovanie umožňuje organizáciám identifikovať a riešiť bezpečnostné slabiny skôr, ako ich zneužijú zlomyseľní aktéri. Praktické skúsenosti: Kurzy ako Real World Penetration Testing zahŕňajú praktické laboratórne cvičenia, kde účastníci môžu svoje znalosti aplikovať v reálnych scenároch.

Pre koho?

Školenie Real World Penetration testing je určené pre:
Bezpečnostní profesionáli: Tí, ktorí už pracujú v oblasti informačnej bezpečnosti a chcú rozšíriť svoje znalosti a zručnosti v konkrétnych oblastiach, ako je penetračné testovanie. IT profesionáli: Systémoví a sieťoví administrátori, vývojári softvéru a iní IT odborníci, ktorí chcú získať hlbšie porozumenie bezpečnostných hrozieb a ako ich efektívne riešiť. Personál SOC služieb. Konzultanti a audítori kybernetickej bezpečnosti: Odborníci, ktorí poskytujú rady alebo hodnotenia tretích strán, a potrebujú rozumieť metodikám a technikám penetračného testovania na hlbšej úrovni.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Zlepšená schopnosť identifikovať zraniteľnosti: Účastníci sa naučia, ako používať rôzne nástroje a techniky na odhalenie slabín v IT infraštruktúre, čo je kľúčové pre zabezpečenie systémov pred útočníkmi. Praktické skúsenosti s penetračnými testami: Kurz poskytuje praktické laboratórne cvičenia, ktoré umožňujú účastníkom aplikovať teoretické znalosti v kontrolovanom prostredí. Toto “učenie sa robením” je neoceniteľné a zvyšuje ich sebadôveru pri vykonávaní skutočných penetračných testov. Pripravenosť na kybernetické hrozby: Kurz pomáha účastníkom rozvíjať schopnosti potrebné na rýchlu reakciu na bezpečnostné incidenty a na efektívne zvládanie potenciálnych hrozieb, čo je nevyhnutné pre udržanie bezpečnosti v dynamickom digitálnom prostredí.

ŠKOLENIE PRIPRAVUJE TECHNICKÝCH ŠPECIALISTOV A ODBORNÍKOV NA KYBERNETICKÚ BEZPEČNOSŤ NA VYKONANIE FORENZNEJ ANALÝZY PRE POTREBY INCIDENT RESPONSE

Čo je?

Školenie obsahuje:
Základy digitálnej forensics: Úvod do princípov a praktík digitálnej forensics, vrátane právnych a etických aspektov.
Zachovanie dôkazov: Metódy a techniky zabezpečenia a ochrany digitálnych dôkazov aby zostali nezmenené a mohli byť použité v súdnych sporoch.
Analýza dát: Použitie špecializovaných forenzných nástrojov na extrahovanie a analýzu údajov z rôznych zdrojov ako sú pevné disky, mobilné zariadenia, sieťové záznamy atď.
Pokročilé forenzné techniky: Detailné štúdium techník ako Steganografia, kryptografia a analýza malvéru.
Reporting a prezentácia nálezov: Výuka o tom, ako efektívne prezentovať zistenia z forenznej analýzy súdom alebo iným zainteresovaným stranám.
Prípadové štúdie a simulácie: Reálné prípadové štúdie a simulované scenáre, kde môžu účastníci aplikovať svoje znalosti a zručnosti v praxi.

Prečo?

Absolvovanie kurzu Real World Forensics Analysis ponúka množstvo dôležitých prínosov pre jednotlivcov aj organizácie. Tento druh vzdelávania je kľúčový pre rozvoj zručností, ktoré sú nevyhnutné na efektívne zvládanie bezpečnostných incidentov a posilnenie celkovej obranné schopnosti systémov. Kurz naučí účastníkov, ako správne zachytiť, analyzovať a interpretovať digitálne dáta po bezpečnostnom incidente. Tieto zručnosti sú neoceniteľné pri vyšetrovaní a mitigácii škôd spôsobených útokmi.

Pre koho?

Kurz Real World Forensics Analysis je určený pre odborníkov, ktorí chcú rozvíjať svoje znalosti a zručnosti v oblasti digitálnej forensics ako sú bezpečnostní profesionáli, členovia SOC tímov, právnici a právni poradcovia, vládni vyšetrovatelia a zamestnanci bezpečnostných agentúr, nezávislí konzultanti a bezpečnostní audítori.

Prínosy?

Rozšírené forenzné zručnosti: Účastníci získajú hlboké pochopenie o tom, ako zachytiť, analyzovať a interpretovať digitálne dáta v súvislosti s bezpečnostnými incidentmi. Tieto zručnosti sú neoceniteľné pri určovaní príčin a rozsahu kybernetických útokov a iných bezpečnostných porušení.
Lepšia schopnosť reagovať na incidenty. Kurz poskytuje prístup k najnovším technológiam a metodikám v digitálnej forensics, čo umožňuje účastníkom zostať na čele v rýchlo sa meniacom poli kybernetickej bezpečnosti.

ŠKOLENIE JE PRIPRAVÍ TECHNICKÝCH ŠPECIALISTOV A ODBORNÍKOV NA REÁLNE RIEŠENIE KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV V ORGANIZÁCII

Čo je?

Školenie je rozdelené na 4 časti (rovnako ako samotný proces riešenia incidentov):
• Príprava na riešenie bezpečnostného incidentu
• Detekcia a analýza kybernetického incidentu
• Obmedzenie šírenia bezpečnostného incidentu ,Eradication a Obnova
• Systémové zmeny v bezpečnostnom prostredí organizácie
Každá časť je postavená na reálnych prípadoch a zostavená tak, aby účastníkovi školenia dala poznatky a „hands-on“ pri jednotlivých krokoch riešenia bezpečnostného incidentu.
Scenár incidentu, ktorý sa bude počas školenia riešiť je postavený na reálnom prípade APT útoku na nadnárodnú organizáciu.

Prečo?

Kurz poskytuje účastníkom znalosti a zručnosti potrebné na rýchle a efektívne reagovanie na bezpečnostné incidenty. Toto je kriticky dôležité v dnešnej dobe, keď sú kybernetické útoky čoraz častejšie a sofistikovanejšie.
Minimalizácia škôd a nákladov: Správna reakcia na incidenty môže výrazne znížiť výšku škôd spôsobených útokmi a tým obmedziť finančné a reputačné straty pre organizáciu.
Zlepšenie bezpečnostných postupov: Kurz poskytuje podrobné informácie o najlepších praktikách a stratégiách, ktoré pomáhajú organizáciám zlepšiť ich celkové bezpečnostné postupy a politiky.
Kurz zahŕňa scenáre a simulácie, ktoré účastníkom umožňujú prakticky si vyskúšať a zdokonaliť naučené metódy v kontrolovanom prostredí.

Pre koho?

Školenie Real World incident respons je určené pre:
Bezpečnostní odborníci: Tí, ktorí už pracujú v oblasti kybernetickej bezpečnosti a chcú rozšíriť svoje zručnosti v riadení incidentov. Členovia SOC tímov. IT profesionáli: Systémoví a sieťoví administrátori, ktorí potrebujú zvládať a riešiť bezpečnostné incidenty vo svojich sieťach a systémoch. Incident Response Teams (IRT): Členovia tímov reagujúcich na incidenty, ktorí sa špecializujú na rýchlu a efektívnu reakciu na bezpečnostné incidenty v reálnom čase.

Prínosy?

Zlepšené schopnosti detekcie a reakcie: Účastníci sa naučia, ako efektívne identifikovať a reagovať na bezpečnostné incidenty. Získané znalosti pomáhajú rýchlejšie rozpoznať hrozby a adekvátne na ne reagovať, čo je kľúčové pre minimalizáciu škôd a obnovu normálnej prevádzky.
Zníženie nákladov spojených s incidentmi: Efektívna reakcia na incidenty môže výrazne znížiť náklady spojené s narušením operácií, stratou dát a následnými právnymi alebo regulačnými sankciami. Účastníci sa naučia, ako znižovať tieto náklady prostredníctvom rýchlej a organizovanej reakcie.
Komplexné zvládnutie incident response procesu: