KATALÓG SLUŽIEB 2024

NAKIB

AUDIT A GAP ANALÝZY

NÁRODNÁ AKADÉMIA PRE KYBERNETICKÚ
A INFORMAČNÚ BEZPEČNOSŤ

NAKIB.SK

NAKIB

AUDIT A GAP ANALÝZY

Kyber Security
zákon 69 ZoKB

Kyber 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

VYKONANIE AUDITU ALEBO GAP ANALÝZY PODLÁ POŽIADAVIEK KYBER SECURITY 69/2018 ZOKB

Čo je?

Výkon auditu Kyber Security je komplexný proces posudzovania súladu informačného systému a kybernetickej bezpečnosti organizácie s požiadavkami Kyber 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 Kyber 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 Kyber Security prináša viacero benefitov:
Zvýšenie súladu: Zabezpečenie súladu s požiadavkami Kyber 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 Kyber Security je určený pre:
Všetky organizácie: Bez ohľadu na veľkosť alebo typ činnosti, ktoré spracúvajú chránené údaje v súlade s Kyber 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 Kyber 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 Kyber 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 Kyber Security zákonom posilňuje dôveru partnerov a zákazníkov v organizáciu.

VYKONANIE AUDITU ALEBO GAP ANALÝZY PODLÁ POŽIADAVIEK KYBER SECURITY NIS

Čo je?

Výkon auditu Kyber Security podľa Smernice NIS (NIS Directive)
Čo to znamená: Výkon auditu Kyber 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 Kyber 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 Kyber 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 Kyber 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 PODLÁ 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 PODLÁ 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 PODLÁ 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 PODLÁ 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 PODLÁ 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.