



**KATALÓG SLUŽIEB 2024**

**NAKIB**

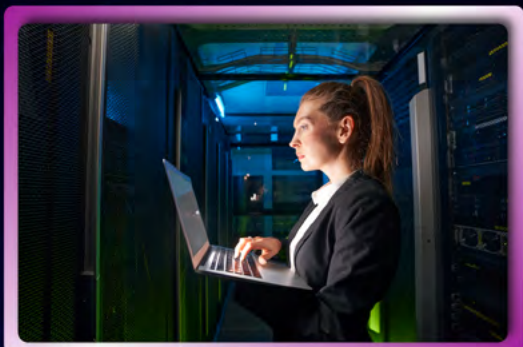
**OUTSOURCOVANÉ ROLE**

**NÁRODNÁ AKADEMIA PRE KYBERNETICKÚ  
A INFORMAČNÚ BEZPEČNOSŤ**

**NAKIB.SK**

# NAKIB

## OUTSOURCOVANÉ ROLE



**Výkon MKB**



**Výkon DPO**



**Výkon IA**



**Výkon SOC Služieb**

**NAKIB.SK**

# NAKIB

## OUTSOURCOVANÉ ROLE

### Výkon MKB



## 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.



# NAKIB

## OUTSOURCOVANÉ ROLE

### Výkon DPO



## 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 efektívnosť 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.

# NAKIB

## OUTSOURCOVANÉ ROLE

# Výkon SOC Služieb



## 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 efektívnosť 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.