Kybernetická bezpečnost

Topical Requirement

Tematické požadavky

The Institute of
Internal Auditors

Tematické požadavky kybernetické bezpečnosti

Mezinárodní rámec profesní praxe (International Professional Practices Framework®) se skládá z Globálních standardů interního auditu (Global Internal Audit Standards™), Tematických požadavků a Globálních návodů. Tematické požadavky jsou závazné a musí se využívat společně se Standardy, které představují požadovaný základ pro praxi.

Tematické požadavky stanovují minimální základ pro audit určitých oblastí rizik a poskytují tak interním auditorům jasná očekávání. Rizikový profil organizace může vyžadovat, aby interní auditoři zvážili další aspekty dané oblasti.

Soulad s Tematickými požadavky zvýší konzistentnost při poskytování služeb interního auditu a zlepší kvalitu a spolehlivost služeb a výsledků interního auditu. Tematické požadavky v konečném důsledku pozdvihují profesi interního auditu.

Interní auditoři musí uplatňovat Tematické požadavky v souladu s Globálními standardy interního auditu. Dodržování Tematických požadavků je povinné pro ujišťovací služby a doporučené pro poradenské služby.

Tematické požadavky se uplatní, pokud je dané téma:

A. Předmětem zakázky v plánu interního auditu.
B. Identifikováno při provádění zakázky.
C. Předmětem žádosti o zakázku, která nebyla zahrnuta v původním plánu interního auditu.

Každý jednotlivý požadavek v Tematických požadavcích musí být posouzen z hlediska jeho uplatnitelnosti a musí o tom být vypracována a uchována evidence. Ne všechny požadavky se musí uplatnit v každé zakázce; pokud jsou ale některé požadavky vynechány, musí být zdokumentováno a uchováno odůvodnění. Soulad s Tematickými požadavky je povinný a bude hodnocen při hodnocení kvality.

Další informace naleznete v Uživatelské příručce k Tematickým požadavkům kybernetické bezpečnosti.

Kybernetická bezpečnost

Národní institut pro standardy a technologie při ministerstvu obchodu USA (NIST) definuje kybernetickou bezpečnost jednoduše jako "schopnost chránit nebo bránit kybernetický

prostor a jeho využívání před kybernetickými útoky". Kybernetická bezpečnost je podmnožinou jí nadřazené informační bezpečnosti, kterou NIST definuje jako "ochranu informací a informačních systémů před neoprávněným přístupem, použitím, vyzrazením, narušením, modifikací nebo zničením s cílem zabezpečit důvěrnost, integritu a dostupnost".

Kybernetická bezpečnost snižuje riziko posílením celkového prostředí řízení a kontroly a ochranou informačních aktiv organizace před neoprávněným přístupem, narušením, změnou nebo zničením. Kybernetické útoky mohou vést k přímým i nepřímým dopadům, které jsou často významné, protože počítače, sítě, programy, data a citlivé informace jsou kritickými komponenty většiny organizací.

Hodnocení a posuzování řízení a správy, řízení rizik a řídicích a kontrolních procesů kybernetické bezpečnosti

Tyto Tematické požadavky poskytují konzistentní a komplexní přístup k posouzení schématu a implementace řízení a správy, řízení rizik a řídicích a kontrolních procesů kybernetické bezpečnosti. Požadavky představují minimální základ pro posuzování kybernetické bezpečnosti organizace.

ŘÍZENÍ A SPRÁVA: Hodnocení a posuzování řízení a správy kybernetické bezpečnosti

Požadavky:

Interní auditoři musí ve vztahu k řízení a správě kybernetické bezpečnosti organizace posoudit následující:

A. Jsou stanoveny a pravidelně aktualizovány formální strategie a cíle kybernetické bezpečnosti. Aktuální informace o plnění cílů kybernetické bezpečnosti jsou pravidelně sdělovány a přezkoumávány orgány společnosti, a to i z hlediska zdrojů potřebných k plnění strategie kybernetické bezpečnosti.

B. Jsou zavedeny a pravidelně aktualizovány zásady a postupy týkající se kybernetické bezpečnosti s cílem posílit kontrolní prostředí.

C. Jsou stanoveny role a odpovědnosti pro plnění cílů kybernetické bezpečnosti a existuje proces pravidelného hodnocení znalostí, dovedností a schopností osob, které tyto role zastávají.

D. Příslušné zainteresované subjekty jsou zapojeny do diskuse o existujících zranitelných místech a nových hrozbách v oblasti kybernetické bezpečnosti a jednají podle toho. Mezi zainteresované subjekty patří vrcholové vedení, provoz, oddělení řízení rizik, oddělení lidských zdrojů, právní oddělení, oddělení compliance, dodavatelé a další.

ŘÍZENÍ RIZIK: Hodnocení a posuzování řízení rizik kybernetické bezpečnosti

Požadavky:

Interní auditoři musí ve vztahu k řízení rizik kybernetické bezpečnosti organizace posoudit následující:

A. Procesy hodnocení a řízení rizik v organizaci zahrnují identifikaci, analýzu, zmírňování a monitorování hrozeb kybernetické bezpečnosti a jejich vlivu na dosažení strategických cílů.

B. Řízení rizik kybernetické bezpečnosti probíhá napříč celou organizací a může zahrnovat následující oblasti: informační technologie, systém korporátního řízení rizik, lidské zdroje, právní záležitosti, compliance, provoz, dodavatelský řetězec, účetnictví, finance a další.

C. Jsou stanoveny odpovědnosti v řízení rizik v oblasti kybernetické bezpečnosti, i kdo za ně plně zodpovídá. Je určena osoba nebo tým, který pravidelně monitoruje a podává zprávy o tom, jak jsou rizika kybernetické bezpečnosti řízena, a to i z hlediska zdrojů potřebných ke zmírnění rizik a identifikaci nových hrozeb kybernetické bezpečnosti.

D. Je zaveden proces pro rychlou eskalaci jakéhokoli rizika kybernetické bezpečnosti (vznikajícího nebo již dříve identifikovaného), které dosáhne nepřijatelné úrovně podle zavedených směrnic pro řízení rizik nebo platných právních a regulačních požadavků. Měly by být zohledněny finanční i nefinanční dopady kybernetického bezpečnostního rizika.

E. Je zaveden proces pro informování vedení a zaměstnanců o rizicích kybernetické bezpečnosti a proces, podle kterého vedení pravidelně přezkoumává problémy, mezery, nedostatky nebo selhání kontroly, je včas informováno a schopno zajistit nápravu.

F. Pro případ kybernetického bezpečnostního incidentu má organizace zavedený proces reakce a obnovy, který zahrnuje detekci incidentu, jeho zvládnutí, obnovu a analýzu po incidentu. Proces reakce a obnovy je pravidelně testován.

ŘÍDICÍ A KONTROLNÍ MECHANISMY: Hodnocení a posuzování řídicích a kontrolních procesů kybernetické bezpečnosti

Požadavky:

Interní auditoři musí ve vztahu k řídicím a kontrolním procesům kybernetické bezpečnosti organizace posoudit následující:

A. Je zaveden proces, který zajišťuje zavedení interních kontrolních mechanismů i kontrolních mechanismů u dodavatelů, aby byla chráněna důvěrnost, integrita a dostupnost systémů a dat organizace. Pravidelně se provádí hodnocení, zda kontroly fungují způsobem, který podporuje dosahování cílů kybernetické bezpečnosti organizace a pohotové řešení problémů.

B. Je zaveden proces řízení talentů, který zahrnuje školení pro rozvoj a udržování technických kompetencí souvisejících s operacemi kybernetické bezpečnosti. Tento proces je pravidelně přezkoumáván.

C. Je zaveden proces průběžného monitorování a hlášení vznikajících hrozeb a zranitelností v oblasti kybernetické bezpečnosti, který pomáhá identifikovat, prioritizovat a implementovat příležitosti ke zlepšení kybernetické bezpečnosti.

D. Kybernetická bezpečnost je zahrnuta do řízení životního cyklu (výběr, používání, údržba a vyřazení z provozu) všech prostředků IT, včetně hardwaru, softwaru a služeb dodavatelů.

E. Jsou zavedeny procesy pro posílení kybernetické bezpečnosti, včetně konfigurace, správy zařízení koncových uživatelů, šifrování, bezpečnostního záplatování (patching), správy přístupu uživatelů a monitorování dostupnosti a výkonu. Kybernetická bezpečnost je zohledněna při vývoji softwaru (DevSecOps).

F. Jsou zavedeny kontroly související se sítí, jako jsou kontroly přístupu k síti a segmentace, používání a umístění firewallů, omezení připojení z externích sítí a do nich, virtuální privátní sítě (VPN)/přístup k sítím s nulovou důvěryhodností (ZTNA), kontroly sítí internetu věcí (IoT) a systémy detekce/prevence narušení (IDS a IPS).

G. Pro služby, jako jsou e-mail, internetové prohlížeče, videokonference, zasílání zpráv, sociální média, cloud a protokoly pro sdílení souborů, jsou zavedeny kontroly zabezpečení koncových bodů (endpoint-communication).

O Institutu interních auditorů

Institut interních auditorů (The IIA) je mezinárodní profesní sdružení, které sdružuje více než 255 000 členů po celém světě a udělilo více než 200 000 certifikátů Certified Internal Auditor® (CIA®) po celém světě. Organizace IIA byla založena v roce 1941 a je celosvětově uznávána jako lídr v oblasti standardů, certifikací, vzdělávání, výzkumu a odborného poradenství pro profesi interního auditu. Další informace naleznete na adrese www.theiia.org.

Autorská práva

únor 2025

The Institute of Internal Auditors

Globální ústředí
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Telefon: +1-407-937-1111
Fax: +1-407-937-1101