

Uafhængig revisorerklæring

Afvigelsesrapport – ISAE 3000

13.02.2024

Introduktion

Denne rapport giver et overblik over fundene fra ISAE 3000 den uafhængige assurance-audit for perioden 1. januar 2023 til 31. december 2023 og beskriver de foranstaltninger, IT Relation har implementeret som respons. Vores mål er at forfine vores operationelle processer og servicelevering for at stemme overens med branchestandarder. Dette dokument deler de skridt, vi har taget for at adressere auditets observationer, og fremhæver vores indsats for at forbedre vores praksis og opretholde en høj kvalitet af service for vores kunder og interessenter.

Auditet har tilbudt værdifuld indsigt for forbedring og udvikling. Inden for dette dokument vil du finde en gennemgang af de korrigerende handlinger, vi har sat i værk efter auditets anbefalinger. Disse tiltag er en del af vores løbende strategi for at forbedre vores tjenester, øge operationel effektivitet og styrke vores sikkerhedsprotokoller.

Vi ser auditets resultater som en chance for at forbedre vores organisation. Der er taget hurtige skridt til at adressere de identificerede forbedringsområder, med en forpligtelse til at forfølge langsigtede initiativer, der sigter mod at øge vores operationelle effektivitet. Denne rapport forklarer vores tilgang til auditets fund og vores strategi for løbende forbedring på tværs af virksomheden.

Vi opfordrer vores interessenter, kunder og partnere til at gennemgå denne rapport. Den demonstrerer vores forpligtelse til at være åbne, ansvarlige og fokuserede på at forbedre vores IT-tjenester og løsninger. Gennem en positiv respons på feedback og en dedikation til kvalitet søger IT Relation at opretholde og forbedre vores rolle i IT-sektoren.

Afvigelsesrapport

B.6 Fejlagtige adgangsrettigheder

Root Cause:

Observationen identificerede forkerte rolletildelinger til medarbejdere i forbindelse med overførslen af arbejdsrelaterede opgaver. Dette problem opstod, da IT Relation kopierede en eksisterende rolleprofil for at tildele den til en medarbejder, som skulle overtage en andens opgaver. Den kopierede rolleprofil indeholdte adgangsrettigheder, som ikke var nødvendige for den nye tildeltes tiltænkte ansvarsområder. Denne misjustering skete på grund af direkte kopiering af rolleprofiler uden tilstrækkelig tilpasning af adgangsrettighederne for at matche de specifikke behov for de nye opgave tildelinger.

Korrigerende Handlinger:

Vi har implementeret en robust kontrolmekanisme for at sikre nøjagtigheden af tildelingen af adgangsrettigheder. Denne kontrolproces er uderligere blevet forstærket både med hensyn til frekvens og omfang, med det formål nøje at korrigere og forhindre enhver gentagelse af forkert tildeling af adgangsrettigheder.

Ansvarlige for udførelse af korrigerende:

User Management-afdelingen hos IT Relation er blevet pålagt at forbedre de eksisterende procedure for at forhindre gentagelse af lignende hændelse. Derudover er Compliance & Security-afdelingen tildelt ansvaret for at overvåge implementeringen af de nyintroducerede kontrolaktiviteter for at sikre deres effektive integration og færdiggørelse.

Status:

Observationen er blevet rettet, de korrigerende handlinger implementeret, og kontrolaktiviteterne fungerer løbende.

I.3 Sikkerhedshændelsesprocedure

Root Cause:

Root Cause til observationen stammer fra håndteringen af et sikkerhedsincident, som ikke levede op til de forventede standarder for kvalitet og tilstrækkelighed, som er beskrevet i IT Relations sikkerhedshændelsesprocedure. Denne mangel førte til forsinket feedback, kommunikation og respons i forbindelse med enkelte sikkerhedshændelser. Det underliggende problem var procedurens utilstrækkelighed, specifikt manglen på en omfattende vurdering af forskellige faktorer, der er nødvendige for nøjagtigt at bestemme alvorligheden og omfanget af sikkerhedshændelser.

Korrigerende Handlinger:

Vi har forfinet vores procedure for at sikre, at de kvalitative trin, der er nødvendige for at fastlå alvorligheden af en sikkerhedshændelse, nu er en integreret del af proceduren i stedet for at afhænge af den subjektive vurdering fra den enkelte medarbejder, der håndterer sikkerhedshændelsen. Derudover har vi udviklet nye skabloner for sikkerhedshændelser for at inkorporere disse justinger. For yderligere at forbedre vores respons på sikkerhedshændelser har vi også iværksat omfattende træning rettet mod at forbedre den korrekte håndtering af sådanne hændelser.

Ansvarlige for udførelse af korrigerende:

Compliance & Security-afdelingen er blevet pålagt at forbedre proceduren for at tilsikre en fortsat tilstrækkelig håndtering af sikkerhedshændelser.

Status:

Observationen er blevet rettet, de korrigerende handlinger implementeret, og den nyintroducerede procedure er operationel.

Konklusion

Denne rapport præsenterer fundene fra ISAE 3000 den uafhængige assurance-audit, herunder de identificerede problemer, deres årsager og de skridt, vores organisation har taget for at adressere dem. Som reaktion har vi foretaget justeringer af vores sikkerhedsprocedurer, roller og uddannelsesprogrammer.

Vores respons har inkluderet indførelsen af stærkere kontrolmekanismer og opdateringer til vores processer for håndtering af sikkerhedshændelser. Disse handlinger er en del af vores løbende bestræbelser på at udvikle os og reagere på de skiftende krav inden for IT-sikkerhed.

For at konkludere ser vi resultaterne af auditet som en chance for at lære og vokse, og vi forbliver forpligtede til at opretholde høje standarder for service og til at tjene vores fællesskabs tillid.

Kontakt

Hvis der er behov for yderligere information, eller hvis rapporten giver anledning til yderligere spørgsmål, bedes du rette dine forespørgsler til Compliance & Security afdelingen hos itm8 på: compliance@itm8.com