

Begrundelser for afvigelserne i Visma TIME m SYSTEM's ISAE3000 erklæring 2024

AD B.6 - Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor:

Ved gennemgang af brugeradgange blev det konstateret, at flere brugere havde adgang til personoplysninger end hvad der kunne dokumenteres som godkendt. Det blev oplyst, at adgangen var arbejdsbetinget, men at den formelle godkendelse ikke var dokumenteret.

Vores begrundelse:

Afvigelsen skyldes manglende dokumentation af allerede eksisterende arbejdsbetingede adgange. Der er etableret procedurer for tildeling og afbrydelse af brugeradgange til personoplysninger, som sikrer, at adgange gives på baggrund af et arbejdsbetinget behov. Afvigelsen relaterer sig til dokumentationsniveauet for allerede eksisterende adgange, ikke til fravær af kontrol. For at styrke den fremadrettede sporbarhed er den eksisterende praksis blevet suppleret med en mere systematisk tilgang til registrering og validering af godkendelser. Dette sikrer, at alle brugeradgange kan dokumenteres fuldt ud i fremtidige erklæringer.

AD B.9 Der er etableret logning i systemer, databaser og netværk af følgende forhold. Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.

Det blev konstateret, at nogle af de logfiler, der blev fremlagt til dokumentation, dækkede en periode efter den aktuelle erklæringsperiode. Dette skyldtes opsætning af opbevaringsperiode i systemet.

Vores begrundelse:

Afvigelsen er af teknisk karakter og skyldes, at logsystemets standardkonfiguration overskrev ældre logdata før revisionens start. Der er ikke sket ændringer i logningsprocedurerne, og der er fortsat implementeret og aktiveret tekniske kontroller, der sikrer løbende logning og opfølgning. For at forbedre tilgængeligheden af relevant dokumentation fremadrettet, har vi justeret processerne for arkivering og genfindning af logs, så revisionsrelevante perioder sikres særskilt.

AD B.12 Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.

12 (tolv) ud af 23 (treogtyve) ændringer kunne ikke dokumenteres testet af kunden, da systemets opbevaringsperiode for denne dokumentation var overskredet.

Vores begrundelse:

Afvigelsen skyldes en teknisk begrænsning i systemets dokumentationsmodul, som automatisk sletter test- og godkendelsesdokumentation efter en given periode. Vi gør opmærksom på, at der ikke er sket ændringer i de procedurer, der skal sikre test og godkendelse, og at disse procedurer er blevet fulgt.

For at sikre bedre tilgængelighed af relevant dokumentation fremover er der foretaget justeringer i den måde ændringsdata arkiveres og fremsøges på. Dette skal understøtte, at dokumentationen for kundetest og godkendelse bevares tilstrækkeligt længe og let kan fremfindes i forbindelse med kommende revisioner

AD C.3 medarbejdere i forbindelse med ansættelse. Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.

Screeningsmateriale for 2 (to) ud af 3 (tre) nyansatte var ikke modtaget rettidigt i forbindelse med ansættelse.

Vores begrundelse:

Afvigelsen skyldes, at screeningsmateriale i enkelte tilfælde ikke er blevet indhentet rettidigt pga. administrative forsinkelser. Vi gør opmærksom på, at der foreligger formaliserede procedurer for efterprøvning ved ansættelse, og at screeningskravene er uændrede siden forrige erklæringsperiode. For at sikre endnu bedre tilgængelighed og sporbarhed i dokumentationen fremadrettet, er processerne for registrering og opbevaring af screeningsmateriale blevet justeret, så relevant dokumentation altid kan tilgås rettidigt i forbindelse med revision og kontrol.

AD C.7 Der gennemføres løbende awarenessstræning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.

Flere ansatte havde adgang til personoplysninger, end der var dokumenteret gennemført awarenessstræning for.

Vores begrundelse:

Awarenessstræning er en obligatorisk del af vores informationssikkerhedsprogram og indgår som et fast element i medarbejdernes onboarding og løbende kompetenceudvikling. For at sikre fuld sporbarhed i dokumentationen af gennemført træning, er der foretaget en styrkelse af vores registreringspraksis. Det sikrer, at træningsstatus altid er opdateret og kan dokumenteres i forbindelse med revision – i tråd med den gældende sikkerhedspolitik.