ØKONOMISTYRELSEN

Tjekliste for opfyldelse af minimumskrav til løsningsarkitektur for systemer, der afleder udbetalinger

I nedenstående tabel redegøres der for mTimes opfyldelse af minimumskrav (implementering i BM).

Nr.	Minimumskrav	Bemærkninger ved myndighed	Bemærkninger ved leverandør
		Lovkrav	
2.1	Overholdelse af gældende regnskabsrelateret lovgivning	Opfyldt Økonomistyrelsen har fastlagt, at den relevante regnskabsrelaterede lovgivning fsva. mTime er 1) Rigsrevisorloven og 2) regnskabsbekendtgørelsen. Relevante paragraffer fremgår af reference implementeringen. *1. Rigsrevisorloven.* Kravet er opfyldt, da Rigsrevisor har adgang til at udtale sig om forhold med betydning for revisionen. Rigsrevisionen er bekendt med brugen af mTime og har revideret elementer i relation hertil. *2. Regnskabsbekendtgørelsen.* Kravet er opfyldt. Reference implementeringen angiver følgende relevante paragraffer. Det bemærkes, at mTime ikke er et udbetalingssystem, men alene betalingsafledende. • §21.2: Der er funktionsadskillelse mellem udvikling, drift og kontrol overfor regnskabsmæssig registrering og betaling, da sidstnævnte	

Nr.	Minimumskrav	Bemærkninger ved myndighed	Bemærkninger ved leverandør
		dele er i Statens Administration • §24: mTime er ikke udbetalingssystem. Der er funktionsadskillelse mellem regnskabsmæssig registrering og betaling. Statens Administration indestår for dette • §25: Relevante økonomiske hændelser registreres i regnskabet. Tidsregistrering afsluttes månedligt. Ydelser udbetales efter faste kadencer. • §27: Betalinger mv. dokumenteres med udtræk fra mTime, som udgør bilag og dokumentation. • §28,2: Der foretages kontrol af udbetalinger. Alle registreringer skal godkendes. Der henvises derudover til lønkontrolplanen. • §29: mTime er ikke udbetalingssystem. Betalinger sker i de fællesstatslige systemer. • §44: Regnskabsmateriale opbevares i minimum 5 år jf. §27. Data fra mTime opbevares også i minimum 5 år.	

Nr.	Minimumskrav	Bemærkninger ved myndighed	Bemærkninger ved leverandør
		• §45: Data fra mTime opbevares i Danmark. mTime driftes hos SIT, hvis datacentre ligger i Danmark. • §49,2: Ikke relevant	
2.2	Overholdelse af gældende GDPR-lovgivning	Alle underpunkter bortset fra to vurderes opfyldt. BM mangler at lave 1) en risikovurdering af anvendelse af produktionsdata som testdata og 2) en vurdering af samme op imod artikel 5's princip om dataminimering. **Kompenserende handling**: Disse vil blive vurderet i løbet af 2022. Vurdering af delkrav er vedlagt i bilag a).	-
Systemkrav			
2.3	Restriktiv adgangsstyring	Passwords: Opfyldt. Adgang til systemet foregår ved hjælp af SITs SSO løsning, hvor der er kvalitative krav til passwords, sløring af indtastede oplysninger, registrering af fejlede log-on forsøg og nedlukning af sessioner uden aktivitet. Passwords lagres og overføres ikke. Der anvendes flerfaktor autentifikation for medarbejdere i TIMEmSYSTEM, men ikke for administratorer i BM. OES har vurderet, at det er tilstrækkeligt, når SITs SSO anvendes, og der er flerfaktor autentifikation ved ekstern adgang.	

Nr.	Minimumskrav	Bemærkninger ved myndighed	Bemærkninger ved leverandør
		Autorisation: Ikke opfyldt: Der er politik for adgangsstyring i BM, opdelte rettigheder, mulighed for kun at læse, brugere med privilegerede rettigheder har ikke adgang til kildekode. Kun brugere med særlige rettigheder kan tildele rettigheder. Administratorer kan godkende egne og andres timer uden yderligere godkendelser. Det skal enten håndteres gennem manuelle kontroller eller gennem implementering af 4-øjneprincip i systemet. Sidstnævnte foretrækkes. Se også 2.12. BM afventer løsningsforslag fra TMS pba. opstartsmøde. **Kompenserende handling**: Arbejdsgruppe bestående af TMS og ministerier afdækker mulighed for udvikle 4-øjnefunktionalitet. HR overvejer pt. om der er et behov for at indføres manuelle kontroller eller ej i den mellemliggende periode.	TMS har afholdt opstartsmøde med henblik på at udvikle 4-øjneprincip. Indledende vurdering er et omfang på 15-20 timer.
2.4	Pålidelig backup og genskabelse	Opfyldt. FM fører tilsyn med kvaliteten af SIT's backup, herunder at den er tilstrækkelig for almindelige administrative behov. OES har vurderet at SIT's backup svarer til Navision Stats og er tilstrækkelig.	

Nr.	Minimumskrav	Bemærkninger ved myndighed	Bemærkninger ved leverandør
2.5	Sikring af adgang til kildekode	Opfyldt	Efter TimeMSystems opfattelse er ovenstående dækket af ISAE3000 i erklæringen fra 2020 i de to afsnit ændringsstyring og risikovurdering. Der benyttes GIT og JIRA til denne håndtering, hvor de nødvendige krav er indarbejdet i. Disse produkter kan ikke benyttes uden at Begrænsning af adgang, Forgrening, Frekvent kode-review, Logning af ændringer og versionsstyring er indarbejdet. Ingen brugere hos kunden har adgang til kildekode.
2.6	Sammenhængende systemdokumentation	Opfyldt ISAE 3000 erklæring dækker ændringsstyring.	TIMEmSYSTEM vurderer, at nedenstående understøtter behovet for sammenhængende systemdokumentation samt at kravene i vejledningen er dækket af en ISAE 3000 erklæring. Alle 7 punkter beskrevet i vejledningens afsnit om generisk implementering er overholdt: • TIMEmSYSTEM anvender et workflow, der indeholder en procesbeskrivelse i tilfælde af fejl, som er fundet i produktionsmiljøet, eller ved ændringsønsker, der kommer fra en kunde og som kræver en koderettelse. Procesbeskrivelsen beskriver flowet mellem supportteamet, udviklingsteamet og testteamet. • Kunder kan se deres igangværende sager i Kundecenteret, herunder også udviklingsopgaver.

Nr.	Minimumskrav	Bemærkninger ved myndighed	Bemærkninger ved leverandør
			• I Release Notes kan kunder se, hvad der er sket af ændringer i en given version samt hvilke generelle kendte fejl som findes i systemet. • Der udarbejdes de nødvendige brugervejledninger, og de bliver løbende opdateret.
2.7	Robust RPA implementering	Ikke relevant. Der anvendes ikke robotteknologi.	
Applikationskrav			
2.8	Påkrævet logning	Opfyldt. Dækket af ISAE3000 og ISRS erklæring vedrørende TIMEmSYSTEM. Alle krav nævnt under "generisk implementering" er relevante. "Udbetalingsdata" dækker timeregistreringer, mens "handlinger relateret til udbetalingsprocessen" omfatter godkendelser.	TMS vurderer, at alle kravene oplistet i vejledningens afsnit om "generisk implementering" er opfyldt. Det dokumenteres i ISAE 3000 erklæringen.
2.9	Tydeligt transaktionsspor	Opfyldt.	TMS vurderer, at det er opfyldt, idet der er transaktionsspor for de tilkøbte og anvendte dele af mTime. Dvs. aktiviteter i selve systemet for alle kunder, og aktiviteter i SLS-integrationen, hvis det er tilkøbt.
2.10	Datakonsistens og låsning	Opfyldt	Som svar i 2.9, dvs. opfyldt, idet der er datakonsistens og låsning for de tilkøbte og anvendte dele af mTime. Hvis der benyttes SLS integration, så er der fuld transaktionsspor og datakonsistens.

Nr.	Minimumskrav	Bemærkninger ved myndighed	Bemærkninger ved leverandør
			Data bliver låst i forbindelse med brugergodkendelse af opgørelse. Opgørelsen skal endvidere være personaleledergodkendt før, at den kan frigives til SLS. Hvis opgørelsen genåbnes så sker der en logning af dette, og hvis der er forskel i beregningsgrundlaget til SLS, så fremkommer der en ny post i SLS engangsløndele modulet. Hvis man ikke har integration til SLS, men benytter output fra HR-løn statistikken, så stopper datakonsistens og låsning, når statistik til HR-løn bliver trukket. Der skal derfor være interne procedurer fra data forlader mTIME til de indtastes i SLS.
2.11	Ingen undtagelser fra produktstrategien	Uafklaret/ikke opfyldt. Det er svært at vurdere ansvarsfordelingen mellem kunde og leverandør. Det må i udgangspunktet være kundens ansvar, ikke at bestille funktionalitet, der kan undermindre systemets integritet i forhold til den overordnede målsætning om at undgå svig. Leverandøren kan evt. påvirke kundens valg i den rigtige retning, jf. TIMEmSYSTEMs forslag. **Kompenserende handling**: BM vil initiere møde med OES i 2022, hvor dette kan blive afklaret.	TIMEmSYSTEM vil undersøge, om der kan komme et felt i change-request. Feltet skal tydeliggøre, om kunden er ved at bestille en ændring, der udgør en undtagelse eller afvigelse, der kan påvirke systemets sikkerhed i forhold til svig. Der kan være tale om ændringer relateret til fx timegodkendelser, registreringer eller statistik modul, som kræver særligt grundig godkendelse. TIMEmSYSTEM vil komme med et forslag til, hvilke punkter, det kan dreje sig om.
2.12	Tvungen funktionsadskillelse	Ikke opfyldt. Administratorer kan godkende egne og andres timer uden yderligere godkendelser. Det skal	Der er de muligheder som er angivet i TIMEmSYTEMs quickguide til roller og rettigheder,

Nr.	Minimumskrav	Bemærkninger ved myndighed	Bemærkninger ved leverandør
		enten håndteres gennem manuelle kontroller af loggen eller gennem implementering af 4-øjneprincip i systemet. **Kompenserende handling**: Se afsnit 2.3	hvis der er ønske om funktionalitet som ikke er til stede i dag, så er vi åbne for at se på dette. Det er eksempelvis muligt at en administrator kan foretage registreringer og godkende dem selv. Dog er det ikke muligt at godkende disse til udbetaling i SLS, når der anvendes engangsløndele i mTIME. Det er muligt i et mVIEW at se, hvem der har foretaget en registrering og hvem der har godkendt denne.
2.13	End-to-end udbetalingskontrol	Opfyldt. BM udfører kontroller på baggrund af lønkontrolplan ud fra systemets rapporter.	
2.14	Sikker udbetaling via Nemkonto	Ikke relevant. Der sker ikke udbetaling via systemet.	
Tekniske krav			
2.15	Overholdelse af tekniske minimumskrav, jf. sikkerdigital.dk	Opfyldt Patchning og opdatering OS: styres af SIT, da mTime kører på driftsmodel 1a som shared service.	Patchning og opdatering applikation: mTime laver efterprøvning af sårbarheder og laver nye releases, når det er påkrævet.
2.16	Kryptering af betalingsdata ved udveksling	Ikke relevant BM benytter pt. ikke mulighed for integration til SLS. Integrationen til SLS anvender https og TLS protokol ved overførsler til SLS Webservice, og opfylder ifølge OES kravene.	

Nr.	Minimumskrav	Bemærkninger ved myndighed	Bemærkninger ved leverandør
2.17	Blokering for SQL-injektion	Opfyldt.	TIMEmSYSTEM benytter systemer (Burpsuite og Polaris) til løbende automatiske screeninger og kontrol af SQL injections. Dette er en del af Vismas "Visma Application Security Program", også kaldet VASP. VASP er et skræddersyet sikkerhedsprogram baseret på førende industristandarder og bedste praksis og indlejret direkte i vores produktionssystemer.