Security en verantwoording requirements
Europese aanbesteding: technisch beheer OHI

Afdeling: Expertisecentrum ICT en IT Risk & Control
Datum:
Auteur:
Versie:

www.hetcak.nl

1. Inleiding

Het CAK heeft voor het technisch beheer van Oracle Health Insurance (OHI) een aanbestedingsprocedure opgestart.

Het uitbesteden van het technisch beheer houdt in dat het CAK niet dezelfde mate van controle over de beveiliging van het systeem heeft als bij een systeem in eigen beheer. Daarom heeft het CAK een aantal Security Requirements opgesteld waar de uitbestede dienst aan dient te voldoen. Deze lijst aan Requirements bevat de normenkader waar de Opdrachtnemer aan moet voldoen.

2. Dataclassificatie

De dataclassificatie is door de Systeem Eigenaar vastgesteld. Op basis van deze dataclassificatie volgen onderstaande Security Requirements voor het **OHI** systeem.

3. Security Requirements

De systemen en infrastructuur van de leverancier worden gebruikt om het beheer uit te voeren op de CAK omgeving. Vanuit de systemen van de leverancier verkrijgt men toegang tot de data van het CAK. De onderstaande Requirements zijn daarom van belang om inzicht te krijgen in het beveiligingsniveau van de systemen en procedures van de Opdrachtnemer.

Eisen leverancier

ID	Requirement
AVG-01	Opdrachtnemer beschikt over een werkend informatiebeveiligingsmanagement-systeem. De aangeboden services zijn opgenomen binnen de scope van het ISMS. (ISO 27001 of gelijkwaardig is hiervoor een goede basis. Zie hoofdstuk 4.)
AVG-07	De Opdrachtnemer zal een (CAK) Verwerkersovereenkomst afsluiten met het CAK.
ALG-01	Het CAK is gerechtigd, met inachtneming van een vooraankondiging, een audit op voor het CAK relevante systemen bij de leverancier uit te (laten) voeren.
ALG-02	Opdrachtnemer beschikt over een werkende procedure Meldplicht datalekken.
B.02	Tussen het CAK en de Opdrachtnemer behoren de informatiebeveiligingseisen, en periodieke actualisering daarvan, te worden overeengekomen. Deze actualisering dient binnen redelijke termijn kosteloos te worden uitgevoerd.
ACC-01	De Opdrachtnemer krijgt toegang tot de CAK omgeving via een Remote Access portaal met 2-factor authenticatie. De details hiervan zijn uitgewerkt in de “Remote beheer security richtlijn CAK”.

Account en wachtwoord vereisten

ID	Requirement
WEB-02	Indien applicaties communiceren met databases of externe systemen dan zijn de hiervoor gebruikte accounts en wachtwoorden voorzien van een sterk wachtwoord.
WEB-03	Serviceaccounts die ten behoeve van de applicatie binnen het besturingssysteem aangemaakt moeten worden, hebben geen interactieve login rechten (tot terminal server sessies).
U.05	Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.

Kwetsbaarheden beheer / updaten

ID	Requirement
WEB-04	De gehele omgeving is (en blijft) voorzien van de meest recente securityupdates zoals aanbevolen door de leverancier of ontwikkelaar van de gebruikte software.
U.01	De Opdrachtnemer behoort de klant te adviseren met marktontwikkelingen en kennis van (de leeftijd van) applicaties en technische softwarestack over strategische ontwikkeling en innovatieve keuzes voor het ontwikkelen en onderhouden van informatiesystemen in het applicatielandschap.
C.03	Patchmanagement behoort procesmatig en procedureel uitgevoerd te worden, dat tijdig vanuit externe bibliotheken informatie wordt ingewonnen over technische kwetsbaarheden van de gebruikte code, zodat zo snel mogelijk de laatste (beveiligings-) patches kunnen worden geïnstalleerd.

Uitwisseling gegevens

ID	Requirement
WEB-05	Indien de systemen van de Opdrachtnemer gegevens uitwisselen met de applicatie van Opdrachtgever dan is deze gegevensuitwisseling door middel van encryptie beveiligd tegen ongeautoriseerd afluisteren of wijzigen.

Intrusion detection

ID	Requirement
WEB-14	Opdrachtnemer heeft maatregelen getroffen om inbraken op haar systemen te detecteren.

Rapportage

ID	Requirement
RAP-01	CAK ontvangt per kwartaal een voor het CAK relevant overzicht met (security) incidenten van de gebruikte systemen van Opdrachtnemer.

Inrichting en beheer servers

	Requirement
SSD-1	De software en het platform van de Opdrachtnemer zijn geconfigureerd volgens de marktconforme hardeningsrichtlijnen. Het configureren is procesmatig en procedureel ingericht.
SSD-2	Te beschermen gegevens worden veilig opgeslagen in databases of bestanden, waarbij zeer gevoelige gegevens worden versleuteld. Opslag vindt alleen plaats als noodzakelijk.
SSD-30	In de applicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.
WEB-11	Back-ups waarop CAK data aanwezig is zijn met encryptie beveiligd. Enkel geautoriseerde beheerders hebben toegang tot deze back-ups.
WEB-19	Back-ups waarop CAK data aanwezig is zijn tijdens opslag en transport dusdanig beschermd dat enkel geautoriseerde beheerders toegang tot deze backups.
U.03	De Opdrachtnemer behoort processen, procedures en beheersmaatregelen te documenteren, te implementeren en te handhaven.
U.06	Richtlijnen en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van beheer op afstand van servers.
C.02	Technische serveromgevingen behoren maandelijks te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor servers en besturingssystemen.

Logging

ID	Requirement
C.04	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
C.03	Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.
C.05	De organisatie reviewed/analyseert regelmatig de logbestanden om onjuist gebruik en verdachte activiteiten op servers en besturingssystemen vast te stellen en bevindingen aan het management te rapporteren.

4. Verantwoording requirements en bewijslast

Aangezien het CAK ten behoeve van de bestuurlijke verantwoording bewijslast dient aan te leveren voor het betrouwbaar verwerken van gegevens, dient de Opdrachtnemer:

- De IT General Controls te hebben ingericht voor de geleverde diensten conform de beheersdoelstellingen van sectie 5.
- Periodiek (minimaal jaarlijks) bewijsstukken van gedane controles op te leveren waaruit blijkt dat de beheersdoelstellingen van sectie 5 zijn voldaan.

Afspraken over het aanleveren van de bewijslast zijn nader met Opdrachtgever overeen te komen. Daarbij dient Opdrachtnemer rekening te houden met een afstemmingsperiode waarin Opdrachtgever initieel geleverde bewijslast beoordeelt en Opdrachtnemer deze waar nodig aanvult. Als alternatief op het aanleveren van bewijslast, kan de Opdrachtnemer ook jaarlijks een ISAE 3402 Type II opleveren die voldoet aan de volgende eisen:

- Is minimaal gelijkwaardig aan de beheersdoelstellingen van sectie 5 ten aanzien van de overeengekomen dienstverlening.
- De werkingsperiode dekt het volledige kalenderjaar, eventueel in combinatie met bridge letter.
- De beheersmaatregelen voor relevante onderaannemers indien van toepassing.

De Opdrachtnemer dient akkoord te gaan met de aanlevering van bovenstaande stukken op jaarlijkse basis zodat het CAK de aantoonbaar de kwaliteit kan borgen en verantwoorden.

5. Beheersdoelstellingen IT General Controls

Logische Toegangsbeheer (LTB)	
LTBC01	Gebruikers- en beheerders hebben alleen de toegangsrechten die voor hun functie noodzakelijk zijn (need to have principe en need to know).
LTBC02	Gebruikersaccounts en toegangsrechten zijn geautoriseerd.
LTBC03	Gebruikers toegangsrechten worden periodiek geëvalueerd.
LTBC04	Personeelsmutaties worden tijdig verwerkt in de toegangsrechten.
LTBC05	Beheeraccounts en generieke accounts zijn zo veel mogelijk beperkt en verklaard.
LTBC06	Indien aanwezig, kunnen niet persoonsgebonden (generieke) accounts met beheerdersrechten alleen toegepast worden middels een noodprocedure.
LTBC07	Directe (schrijf) toegang tot bedrijfskritische databases is alleen beschikbaar voor een beperkte groep personen welke geen onderdeel uit maken van de gebruikersorganisatie.
LTBC09	Sterke authenticatiemiddelen (bijvoorbeeld wachtwoorden) en procedures zorgen dat toegang is beperkt.
LTBC14a	Kritische (handmatige) activiteiten door systemen en (priviledged)gebruikers dienen te worden vastgelegd middels logging.
LTBC14b	Onverwachte activiteiten door systemen en (priviledged) gebruikers worden nader onderzocht en actie op ondernomen.
Wijzigingsbeheerproces (WBP)	
WBPC01	Alle wijzigingen zijn vooraf geautoriseerd.
WBPC02	Alleen geteste en geaccepteerde wijzigingen worden in productie genomen, door hiertoe bevoegde gebruikers.
WBPC03	Spoedwijzigingen zijn achteraf geautoriseerd.
WBPC04	Er bestaat functiescheiding tussen ontwikkeling en productie. (Het is niet mogelijk om door één persoon zelfstandig een wijziging door te voeren)
WBPC07	Een testomgeving is beschikbaar die representatief is voor de productieomgeving.