Bijlage: Detailbevindingen IT

	Onderdeel	Bevinding
6.	User Access: Superusers (functioneel beheerders)	Het functioneel beheren van de applicatie is momenteel belegd bij uw assistent controllers. De functioneel beheerders kunnen door hun rechten ingerichte functiescheidingen doorbreken en kunnen functionele instellingen binnen AFAS aanpassen; dit is ook noodzakelijk om de applicatie te kunnen beheersen. Wij adviseren u om enkele kritieke activiteiten te definiëren, zoals het muteren van crediteurstamgegevens, en periodiek te toetsen of deze kritieke activiteiten niet (onterecht) zijn uitgevoerd door uw functioneel beheerders. Indien er sprake is van generieke accounts (zoals testaccounts) met vergevorderde rechten adviseren wij u om de logging van deze accounts te betrekken in de periodieke review.
7.	Wijzigingsbeheer	Aangezien er sprake is van een cloudoplossing ligt het algemene onderhoud van de applicatie bij uw softwareleverancier AFAS. Desalniettemin liggen er mogelijkheden bij WNK als gebruikersorganisatie om instellingen in AFAS aan te passen. Dit kan uw interne beheersing beïnvloeden omdat deze instellingen ook betrekking hebben op bijvoorbeeld de inrichting van uw workflows. Wij vernamen dat er nog geen geformaliseerd beleid is voor het wijzigingsbeheer. Dit beleid omvat normaliter het ontwikkelen van wijzigingen in een aparte omgeving, het testen daarvan en het verkrijgen van goedkeuring door de applicatie-eigenaar. Momenteel is het wijzigingsbeheer georganiseerd in een informeel proces. Wij adviseren u om een formeel beleid op te stellen en uw wijzigingsbeheerproces daarop in te richten. Wij adviseren u tevens om het wijzigingsbeheer in te regelen in het reeds bestaande ticketingsysteem, zodat u achteraf door middel van de documentatie in het ticketingsysteem kunt toetsen of wijzigingen worden doorgevoerd conform het ingestelde beleid. Wij wisselen graag met u van gedachten over de manier waarop u dit praktisch kunt inrichten.
8.	Cybersecurity	Het belang van afdoende cybersecuritymaatregelen neemt toe als gevolg van een grotere afhankelijkheid van IT en aangescherpte wet- en regelgeving (zoals de GDPR). Wij vernamen dat er nog geen beleid is om periodieke pen-tests uit te laten voeren op uw IT-omgeving. Wij adviseren u om bij de eerst volgende actualisatie van uw cyberrisicoanalyse te evalueren of er noodzaak bestaat om aanvullende maatregelen te treffen.