1. **Is het HLD correct?**
   Lastig om in één vraag te beantwoorden of het HLD correct is. Een paar dingen vallen me op, waarvan ik denk dat je het nog verder kan aanscherpen:

- Ik vind de nadruk op ethiek met 3 requirements vrij groot. Je schrijft zelf ook al dat het niet heel gangbaar is dat controls echt over mensen gaan. Als dat echt zo is, dan is ethiek ook minder belangrijk. Wellicht kan je slimmer zijn in het formuleren of structuren. Bijvoorbeeld door de ethische requirements wat in te dikken (naar bijv. 1 requirement) en pas wat later te laten terugkomen.
- Wat ik mis (ook antwoord op vraag 2) is een stukje scoping. In het proces-plaatje ga je direct in op risk identification, terwijl ik denk ik nog een stap voor zit waarbij je naar de scope van je gewenste ICF gaat kijken. AI gaat je daar niet mee helpen, maar om AI goed in te kunnen zetten om een ICF te maken denk ik dat een duidelijke scope van cruciaal belang is. Neem bijvoorbeeld de nieuwe wetgeving Digital Services Act. Daarin staan specifieke eisen waaraan platform-organisaties moeten voldoen. Als je daarvoor een ICF zou willen maken met hulp van AI, is het vooral belangrijk om in stap 1 (scoping) dat duidelijk te maken, en daar de juiste informatie bij te zoeken.
- Dat is ook mijn puntje 3: de documentatie-opsomming die je geeft bij je proces-beschrijving (1.2.1) is in de basis prima, maar ik mis nog de documentatie die echt over het proces gaat waarop een ICF van toepassing kan zijn. Volgens mij door wat slimmer te spelen met een stap “scoping” kan je dat wat beter toespitsen.
- Tenslotte zou het denk ik ook heel goed werken om – wellicht in subhoofdstuk – een voorbeeld uit te werken, van hoe de stappen ongeveer werken in een concrete casus. Je zou bijv. die DSA wet kunnen pakken, maar ook een willekeurig ander afgebakende scope. Volgens mij kan dat helpen om de leesbaarheid en begrijpbaarheid te vergroten.

2. **Is het HLD compleet?**
   Zie antwoorden vraag 1.
3. **Is het HLD duidelijk?**
   Zie antwoorden vraag 1.
4. **Wat verwacht je per stap als output? (In welke vorm is de output?)**
   Volgens mij is uiteindelijk het doel om een ICF te maken, met daarin risico’s en controls beschreven die door medewerkers uitgevoerd kunnen worden.
5. **Hoe kan je goed prompten richting het AI-model?**
   Lastig. Dat verschilt heel erg per stap en de input die je geeft. Bij het identificeren van risico’s stel je andere vragen dan bij het prioriteren van risico’s of het bedenken van aansluitende controls. Het zou leuk/goed kunnen zijn om wat voorbeeld prompts per stap op te nemen.
6. **Zou je eerder kiezen voor een open source AI-model of een betaalde versie en waarom?**
   Volgens mij ontkom je er niet aan om met een “secure” model te werken. Als je gevoelige informatie aan zo’n systeem geeft om tot bijv. een lijst met risico’s te komen, dan is dat vaak gevoelige bedrijfsinformatie die je liever niet in een publieke versie deelt.
7. **Wie exact zou de gebruiker zijn van een systeem dat omschreven is in dit HLD?**
   Combinatie van 1^{e} en 2^{e} lijn. Volgens mij zou een 2^{e} lijn (risico)medewerker goed in staat moeten zijn om het systeem zelf te begrijpen en te bedienen, zodat hij/zij de

“business” (1e lijn) kan ondersteunen met het maken van de ICF voor hun specifieke deelgebied. Het is daarmee een combi dus.

8. **Zijn er verschillen als de gebruiker intern of extern is?**
   Ligt er helemaal aan wat de afspraken zijn met de externe gebruiker. Als het een consultant is in dienst van de organisatie waar de ICF voor gemaakt wordt, is er vaak wel sprake van geheimhouding en is er dus feitelijk geen verschil. Ik zie dan ook alleen maar risico’s op gebied van delen van data / gevoelige (bedrijfs)informatie. Als dat geborgd is, zie ik geen echt verschil.
9. **Zou een systeem zoals omschreven in dit HLD goed genoeg zijn voor jou om te gebruiken?**
   In principe wel, al denk ik dat het cruciaal is om een duidelijke scope te hebben alvorens je zo’n systeem gebruikt. Die stap zou ik – als ik zo’n systeem gebruik – daarom altijd willen zetten. Verder zou ik het natuurlijk eerst goed testen, voor het daadwerkelijk te gebruiken 😊 Ook een tweede collega laten meekijken is denk ik van groot belang. De uitkomsten van het systeem moeten goed gevalideerd worden.