



IT Risk Officer tweede lijn

- WO
- Tilburg
- Finance & Risk(/vakgebieden/finance-risk)
- 34 tot 38 uur
- 5.236 - 7.480

Jouw baan

Bij CZ werken we met betekenis, daadkracht en als één team.

We nemen verantwoordelijkheid, tonen lef, blijven leren en maken impact. Samen zetten we ons elke dag in voor toegankelijke en betaalbare zorg voor iedereen. CZ is één van de grootste zorgverzekeraars van Nederland. Samen met onze 2.600 collega's zorgen wij ervoor dat onze ruim 4 miljoen verzekerden de beste zorg ontvangen. De veranderende omgeving, toenemende technologieafhankelijkheid en hoge eisen vanuit externe toezichthouders maken professioneel risicomanagement cruciaal. Als IT Risk Officer:

- Werk je vanuit de onafhankelijke tweede lijn. Je stelt kaders, adviseert, monitort, toetst en challengeert de eerste lijn op de beheersing van IT-, data- en technologierisico's. Het eigenaarschap voor processen, systemen, controls en verbetermaatregelen blijft daarbij nadrukkelijk in de eerste lijn.
- Ontwikkel en onderhoud je heldere en toepasbare kaders, methodieken en procedures voor IT risk management. Je draagt bij aan de doorontwikkeling van het IT Risk Management-framework, het Control Framework en risicoanalyses en betreft relevante bedrijfsonderdelen om de aansluiting op de praktijk te borgen.
- Beoordeel en duid je risico's rond IT, data, cybersecurity, informatiebeveiliging, cloud, digitale weerbaarheid, AI, technologieverandering, IT-uitbesteding en kritieke leveranciers. Je kijkt daarbij naar de samenhang met processen, datakwaliteit, continuïteit en operationele weerbaarheid.
- Geef je kaders mee voor Risk Control Self Assessments (RCSA's) en beoordeel en challenge je de kwaliteit, volledigheid en onderbouwing van de door de eerste lijn uitgevoerde risicoanalyses. Daarnaast voer of regisseeer je tweedelijns monitoring, reviews en control testing op belangrijke IT-processen en key controls. Je beoordeelt of voorgestelde verbetermaatregelen passend zijn en monitort de opvolging.
- Onderzoek je vanuit tweedelijns perspectief de grondoorzaken en samenhang van incidenten, security-events en issues. Je vertaalt je analyses naar concrete adviezen en challengeert de eerste lijn op structurele verbetering.
- Volg je ontwikkelingen in onder meer DORA, de AI Act en relevante toezichtverwachtingen. Je vertaalt deze naar toepasbare kaders, risicoanalyses en managementinformatie voor CZ.
- Breng je gevraagd en ongevraagd onafhankelijke en onderbouwde adviezen uit over IT-, data- en technologierisico's. Je maakt materiële risico's, tekortkomingen in de beheersing en afwijkingen

van de risicobereidheid tijdig zichtbaar en bespreekt of escaleert deze via de geldende governancelijnen. Samen met je collega's vertaal je complexe risico-informatie naar heldere rapportages voor management, bestuur en externe toezichthouders.

Jouw team

Jij bent van groot belang

Je maakt deel uit van de onafhankelijke tweedelijns Risk Management-functie en werkt nauw samen met Operational Risk Officers, de Financial Risk Officer en de Manager Risk. Vanuit je eigen onafhankelijke rol onderhoud je een breed netwerk binnen onder meer IT, Security, architectuur, data, privacy, procurement, servicemanagement, Compliance, Interne Audit en de verschillende bedrijfsonderdelen. Het is een team waarin je vragen kunt stellen, kennis deelt en samenwerkt aan verdere professionalisering van het risicomanagement.

Dit krijg je van ons

- **Focus op opleiding en ontwikkeling**

Binnen CZ krijg je wekelijks ruimte om je te verdiepen in je vak om zo te werken aan je eigen ontwikkeling.

- **Flexibel werken**

Jij bepaalt waar en wanneer je werkt om zo de beste werk-prive balans te bieden. Natuurlijk wel zo dat je ook nog bereikbaar bent voor je team.

- **Keuzesysteem arbeidsvoorwaarden**

Ieder mens is anders dus jij bepaalt welke arbeidsvoorwaarden voor jou het best passen.

Jouw profiel

Dit neem je mee naar onze organisatie

- Je beschikt over wo werk- en denkniveau en hebt bij voorkeur 3 tot 5 jaar relevante ervaring. Een hbo-opleiding kan eveneens passend zijn wanneer je beschikt over aantoonbaar ruime en relevante ervaring. Een opleiding op het gebied van risk en controlling, informatietechnologie, economie, bedrijfskunde, accountancy, audit of vergelijkbaar sluit goed aan. Certificeringen zoals CISA, CISM of CISSP zijn een pré.
- Je hebt relevante ervaring met IT risk management, IT audit, informatiebeveiliging, technology risk, internal control of vergelijkbare tweede- of derdelijnswerkzaamheden, bij voorkeur binnen een gereguleerde of complexe organisatie. Je bent zelfstandig inzetbaar op meerdere IT-risicithema's en hebt oog voor aanpalende vakgebieden, zoals Compliance, privacy, audit en uitbesteding.
- Je hebt ervaring met of aantoonbare affiniteit met AI en de bijbehorende risico's, bijvoorbeeld op het gebied van uitlegbaarheid, datakwaliteit, privacy, security, governance en veranderende wet- en regelgeving.
- Je bent analytisch sterk, onafhankelijk, rolvast en constructief kritisch. Je houdt vast aan je professionele oordeel en weet met verschillende beïnvloedingsstijlen draagvlak en beweging te creëren.
- Je haalt energie uit het realiseren van verandering, bent nieuwsgierig naar onderliggende oorzaken en begrijpt dat niet alle werkzaamheden planbaar zijn.
- Je bent organisatiesensitief en kunt een stevig en helder gesprek voeren met stakeholders op operationeel, tactisch en managementniveau. Je adviseert zelfstandig op inhoud en proces, bewaakt de rolverdeling tussen de eerste en tweede lijn en herkent wanneer escalatie nodig is.

- Je brengt complexe IT-, data- en technologierisico's mondeling en schriftelijk op een begrijpelijke manier over. Je kunt een coachende rol aannemen en neemt collega's mee in de principes en werkwijzen van risicomanagement, zonder het eigenaarschap van de eerste lijn over te nemen.

Onze vragen

Een motivatiebrief is niet nodig, in plaats daarvan ontvangen we graag jouw antwoord op de volgende drie vragen:

- Welke ervaring heb je met het beoordelen en challengen van IT-, data- of technologierisico's? Beschrijf maximaal 2 voorbeelden en licht toe welke rol je zelf vervulde.
- Beschrijf een situatie waarin je vanuit een onafhankelijke risk-, audit- of controlrol tot een ander oordeel kwam dan de verantwoordelijke eerste lijn. Hoe heb je jouw oordeel onderbouwd, hoe ben je omgegaan met weerstand en wat was het resultaat?
- Welke ervaring of affiniteit heb je met AI en de risico's die daarbij horen, bijvoorbeeld rond uitlegbaarheid, datakwaliteit, privacy, security, governance of veranderende wet- en regelgeving? Geef maximaal 2 voorbeelden en licht toe hoe jij deze kennis hebt toegepast of verder wilt ontwikkelen.