



>Retouradres Postbus 16375 2500 BJ Den Haag

Hogeschool Rotterdam
T.a.v. College van Bestuur
Postbus 25035
3001 HA ROTTERDAM

**Hoger Onderwijs en
Studiefinanciering**
Rijnstraat 50
Den Haag
Postbus 16375
2500 BJ Den Haag
www.rijksoverheid.nl

Onze referentie
32935305

Bijlagen
1.CDHO advies 2022/030

Datum 3 juni 2022
Betreft Besluit macrodoelmatigheid Associate degree Information Security

Als u belang hebt bij dit besluit, dan kunt u hiertegen binnen 6 weken, gerekend vanaf de verzenddatum, bezwaar maken. Stuur uw bezwaarschrift naar DUO, Postbus 30205, 2500 GE Den Haag. U kunt uw bezwaar ook digitaal indienen op www.bezwaarschriftenocw.nl.

Geacht College,

Met uw brief van 6 april 2022, door de Commissie Doelmatigheid Hoger Onderwijs (hierna: CDHO) ontvangen op 6 april 2022, hebt u mij het voornemen voorgelegd om de associate degree-opleiding Information Security als bekostigde opleiding te verzorgen in Rotterdam.

Advies CDHO

De CDHO heeft mij bij brief van 10 mei 2022, kenmerk 2022/030, positief geadviseerd over uw aanvraag. Het advies van de CDHO dat integraal onderdeel uitmaakt van dit besluit, treft u hierbij aan.

Besluit

Gelet op de advisering van de CDHO, het bepaalde in de Wet op het hoger onderwijs en wetenschappelijk onderzoek (hierna: WHW) en in de Regeling macrodoelmatigheid hoger onderwijs (hierna: Regeling), heb ik besloten in te stemmen met uw voornemen om de associate degree-opleiding Information Security als bekostigde opleiding te verzorgen in Rotterdam.

Beoordelingskader

De wettelijke grondslag voor mijn besluitvorming is gelegen in artikel 6.2 van de WHW. Voorts is de Regeling leidraad geweest voor mijn afwegingen.

Motivering

Overeenkomstig het advies van de CDHO, concludeer ik dat uw aanvraag voldoet aan de criteria a en b van artikel 4, eerste lid, van de Regeling. Voor de nadere motivering verwijs ik u naar het genoemde advies van de CDHO.

Croho-procedure

Ingevolge artikel 6.2, negende lid, van de WHW, vervalt dit besluit indien de opleiding niet binnen tien maanden na dagtekening van het besluit is geregistreerd in het Centraal register opleidingen hoger onderwijs. Registratie binnen die termijn is niet eerder mogelijk dan nadat de NVAO over onderhavige opleiding een positief besluit heeft genomen in het kader van de toets nieuwe opleiding.

In verband met de geldigheidsduur van dit besluit, adviseer ik u zo spoedig mogelijk een aanvraag voor een toets nieuwe opleiding in te dienen bij de NVAO. Voor de registratie van uw opleiding kunt u gebruik maken van a-Croho. Mocht u vragen hebben over de registratie, dan kunt u contact opnemen met ssg@duo.nl.

Onze referentie
32935305

Een afschrift van deze brief is gezonden aan de CDHO, de NVAO, de Inspectie van het Onderwijs, DUO-Groningen en de Vereniging Hogescholen.

Met vriendelijke groet,

de minister van Onderwijs, Cultuur en Wetenschap,
Robbert Dijkgraaf,
namens deze,
MT-lid Hoger Onderwijs en Studiefinanciering

Ministerie van Onderwijs, Cultuur en Wetenschap
T.a.v. de Minister
Dhr. dr. R.H. Dijkgraaf
Postbus 16375
2500 BJ DEN HAAG

Postadres
Postbus 85498
2508 CD Den Haag
Bezoekadres
Parkstraat 83
2514 JG Den Haag
T: 070 8505300
W: www.cdho.nl
E: info@cdho.nl

Advies nieuwe opleiding

Onderwerp	Ons Kenmerk	Datum
Nieuwe opleiding Hogeschool Rotterdam Voltijd en deeltijd hbo Associate degree Information Security Rotterdam	2022/030	10/05/2022

Geachte heer Dijkgraaf,

Op 06/04/2022 heeft de Commissie Doelmatigheid Hoger Onderwijs het voornemen ontvangen van de Hogeschool Rotterdam om de hbo Associate degree Information Security als bekostigde opleiding te verzorgen te Rotterdam (brief van 06/04/2022 met kenmerk 2821). De aanvraag was voorzien van alle voor de beoordeling benodigde gegevens en is door de commissie in behandeling genomen.

Advies Commissie Doelmatigheid Hoger Onderwijs

Gelet op het hiernavolgende adviseert de commissie u om positief te besluiten op het verzoek van de Hogeschool Rotterdam om de hbo Associate degree Information Security als bekostigde opleiding te Rotterdam te verzorgen.

Beoordelingskader

De wettelijke grondslag voor dit advies is gelegen in art. 6.2 van de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW). Voorts heeft de Regeling macrodoelmatigheid hoger onderwijs van 20 juni 2018, verder te noemen de Regeling, voor de commissie als leidraad gediend. Het beoordelingskader treft u in de bijlage bij dit advies aan.

Omschrijving van de aanvraag

Aanvrager wil de hbo Associate degree Information Security in Rotterdam aanbieden. Het betreft een Nederlandstalige hbo Associate degree in het Croho onderdeel Techniek. De opleiding omvat 120 studiepunten en zal in voltijd- en in deeltijdvorm worden aangeboden. Het curriculum van de Ad Information Security bestaat uit vier blokken van 30 studiepunten met elk een eigen thema: 'Onboarden & toegang tot data' (semester 1), 'Analyseren en testen van data en systemen' (semester 2), 'Cybersecurity in de praktijk' (semester 3) en 'Integreren en toepassen in de

praktijk' (semester 4). Het laatste blok staat in het teken van het integreren van alle kennis en ervaring en het kunnen toepassen in de praktijk. De opleiding kent twee uitstroomprofielen: IT Security (pentesting, netwerken & cloud) en Governance en Compliance (risicomanagement). De opleiding is gericht op mbo-4 gediplomeerden (primair IT-opleidingen), havo of vwo gediplomeerden en werkende ICT-professionals op mbo-4-niveau. Professionals zonder mbo-4-diploma dienen een toelatingsexamen af te leggen. Afgestudeerden van de Associate degree Information Security komen in aanmerking voor functies als junior security officer, pentester of netwerk-/securityspecialist binnen middelgrote en grote bedrijven en organisaties.

Motivering

De aanvraag voldoet naar mening van de commissie aan de criteria a en b in art. 4 lid 1 van de Regeling.

Beoordeling criterium a

Aanvrager stelt dat de hbo Associate degree Information Security aansluit op een arbeidsmarktbehoefte in combinatie met een maatschappelijke behoefte.

Beoordeling arbeidsmarktbehoefte

Ter onderbouwing van de arbeidsmarktbehoefte aan afgestudeerden van de hbo Associate degree Information Security doet aanvrager een beroep op arbeidsmarktgegevens met betrekking tot het opleidingstype bachelor informatica en de beroepsgroep Databank- en netwerkspecialisten uit ROA's database AIS. Daarnaast verwijst aanvrager naar de spanningsindicator en het dashboard met het maandelijkse overzicht van online gepubliceerde vacatures van het UWV (periode januari 2020-oktober 2021), het Factsheet 'Arbeidsmarkt ICT-beroepen' (juni 2019), het Factsheet 'Arbeidsmarkt Financiële dienstverlening' (augustus 2018), het Factsheet 'Arbeidsmarkt Overheid' (mei 2020) en het Factsheet 'Arbeidsmarkt Zorg' (april 2020) van het UWV, het rapport 'De inventarisatie van acute personeelstekorten en -overschotten' van het UWV (juni 2020) en het overzicht van 'Kansrijke beroepen' van het UWV (juni 2021), het rapport 'Verwachtingen werkgevers voor 2021: indicatie uit werkgeversenquête UWV (1 april 2021) van het UWV, de 'Nationale Beroepengids' (2021), de lijst van 'Hottest Jobs' van Randstad (2021), het 'Emerging Jobs Report the Netherlands' van LinkedIn (2020) en de 'Future of Jobs' van het World Economic Forum (2020), het 'Tendrapport ICT en Creatieve Industrie' van de SBB (2020), het 'Nationaal Techniekpact' (update juni 2021), een aantal bronnen op het gebied van digitalisering binnen het mkb: 'Digitalisering in het mkb' van de Kamer van Koophandel (2019), de 'Cybersecurity Health Check' van Baker Tilly (2019), het 'Cybersecuritybeeld Nederland 2021' van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (2021), het artikel 'Mkb worstelt enorm met de AVG' van ondernemersorganisatie ONL (2019) en het onderzoek 'Privacywetgeving AVG, wanneer ben je compliant?' van de Kamer van Koophandel (2019). Ten slotte verwijst aanvrager naar het onderzoek 'Cybersecurity Talent: the Big Gap in Cyber Protection' van het Digital Transformation Institute van Capgemini (2018). Voor wat betreft de regionale arbeidsmarktbehoefte verwijst aanvrager onder meer naar het rapport 'Regio in Beeld Rijnmond' van het UWV (november 2021) aangevuld met 'Moeilijk vervulbare vacatures: regionaal overzicht' (2019) en het overzicht 'Kansrijke beroepen. Rijnmond' (2021) van het UWV, de 'Economische verkenning Rotterdam 2020. Veranderende economie en groeiende innovatiekracht' (februari 2020) en de 'Economische Verkenning Rotterdam 2021. Effecten van corona op de economie' (2021) en het arbeidsmarktdashboard 'Rijnmondinzicht.nl' en 'Zuid-Holland Inzicht'. Ten slotte heeft aanvrager door onderzoeksbureau Lexnova een kwantitatief en een kwalitatief arbeidsmarktonderzoek laten uitvoeren (2021).

De commissie acht met aanvrager binnen ROA's database AIS het opleidingstype bachelor informatica het meest relevant, omdat onder meer de verwante hbo Ad's ICT, ICT-Beheer, IT Service Management en Informatica in dit opleidingstype zijn opgenomen. ROA typeert de toekomstige arbeidsmarktsituatie voor afgestudeerden van dit opleidingstype als 'goed'. ROA verwacht grote knelpunten in de toekomstige personeelsvoorziening in 2026 (zie tabel 1).

Tabel 1. Arbeidsmarktprognoses opleidingstype bachelor informatica

Opleidingstype	Arbeidsmarktprognose variabele	Indicator	Aantal	Totaal % 6 jr.	Gem. jaarlijks %	Typering
> > Bachelor - informatica	verwachte uitbreidingsvraag tot 2026		6600	7	1.1	erg hoog
> > Bachelor - informatica	verwachte vervangingsvraag tot 2026		15500	17	2.6	gemiddeld
> > Bachelor - informatica	verwachte baanopeningen tot 2026		22100	24	3.6	gemiddeld
> > Bachelor - informatica	verwachte instroom van schoolverlaters tot 2026		15600	17	2.6	gemiddeld
> > Bachelor - informatica	ITKP toekomstige knelpunten personeelsvoorziening in 2026	0.95				groot
> > Bachelor - informatica	ITA toekomstige arbeidsmarktsituatie in 2026	0.95				goed

Bron: ROA AIS

Aanvrager heeft tevens verwezen naar de prognoses voor de beroepsgroep Databank- en netwerkspecialisten, omdat in deze beroepsgroep beroepen vallen waarvoor afgestudeerden van de hbo Associate degree Information Security in aanmerking komen, zoals netwerkspecialisten. Uit de prognoses van het ROA blijkt dat er grote knelpunten in de toekomstige personeelsvoorziening worden verwacht (zie tabel 2).

Tabel 2. Arbeidsmarktprognoses beroepsgroep Databank- en netwerkspecialisten

Beroepsgroep	Arbeidsmarktprognose variabele	Indicator	Aantal	Totaal % 6 jr.	Gem. jaarlijks %	Typering
Databank- en netwerkspecialisten	verwachte uitbreidingsvraag tot 2026		5600	8	1.3	erg hoog
Databank- en netwerkspecialisten	verwachte vervangingsvraag tot 2026		8100	11	1.8	laag
Databank- en netwerkspecialisten	verwachte baanopeningen tot 2026		13800	19	3	gemiddeld
Databank- en netwerkspecialisten	ITKB toekomstige knelpunten beroepsgroep in 2026	0.857				groot

Bron: ROA AIS

Voor wat betreft de regionale prognoses stelt aanvrager dat de gemiddelde jaarlijkse uitbreidingsvraag van de bedrijfssector Specialistische zakelijke dienstverlening in de regio Rijnmond 0,8% bedraagt en van de sector informatie en communicatie 1,2%. Aanvrager constateert dat op regionaal niveau geen gegevens per opleidingstype beschikbaar zijn. Voor de opleidingssubsector bachelor Techniek en ICT waar het opleidingstype Bachelor informatica onder valt wordt de arbeidsmarktsituatie in 2026 getypeerd als 'goed'. De commissie overweegt dat ROA's prognoses over bedrijfssectoren betrekking hebben op zeer uiteenlopende beroepen met zeer uiteenlopende opleidingsniveaus en om die reden weinig zegt over een specifieke arbeidsmarktbehoefte aan afgestudeerden van de aangevraagde opleiding. Gelet hierop laat de commissie de prognose voor de bedrijfssector specialistische zakelijke dienstverlening buiten beschouwing.

Aanvrager verwijst verder naar de spanningsindicator van het UWV in de periode van het vierde kwartaal van 2019 tot en met het tweede kwartaal van 2021 voor de beroepsgroep Databank- en netwerkspecialisten en constateert dat de landelijke arbeidsmarkt voor deze beroepsgroep in deze periode krap tot zeer krap is. De commissie heeft tevens gekeken naar de spanning op de landelijke arbeidsmarkt voor Databank- en netwerkspecialisten in het derde en vierde kwartaal van 2021 en

constateert dat de arbeidsmarkt voor deze beroepsgroep met een spanning van 11,39 respectievelijk 13,12 zeer krap is. De regionale arbeidsmarkt laat hetzelfde beeld zien. De commissie concludeert dat de spanningsindicator blijkt geeft van een arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen Ad Information Security.

Aanvrager verwijst daarnaast naar het dashboard van het UWV met een overzicht van het aantal maandelijks gepubliceerde online vacatures. Aanvrager constateert dat voor het beroep security specialist ICT, dat onder de beroepsgroep Databank- en netwerkspecialisten valt, in de periode tussen januari 2020 en oktober 2021 een stijging van het aantal vacatures van 135 tot 279 (+107%) valt waar te nemen. Voor de gehele beroepsgroep van Databank- en netwerkspecialisten is het aantal vacatures in deze periode volgens het dashboard gegroeid van 2.602 tot 4.275 (+64%). Voor de regio Rijnmond constateert aanvrager in dezelfde periode eveneens een grote stijging van online vacatures voor het beroep Security specialist ICT en voor de gehele beroepsgroep Databank- en netwerkspecialisten. De commissie concludeert dat de stijging van het aantal online vacatures voor het beroep security specialist ICT en de beroepsgroep Databank- en netwerkspecialisten blijkt geeft van een arbeidsmarktbehoefte aan afgestudeerden van de hbo Ad Information Security.

Aanvrager beschrijft verder dat uit het Factsheet 'ICT-beroepen' van het UWV (augustus 2019) volgt dat geen enkele andere beroepsklasse zo'n sterke mate van krapte kent als de beroepsklasse ICT-beroepen. Werkgevers geven aan dat 70% van de ICT-vacatures moeilijk vervulbaar is (p. 1). Een gebrek aan specifieke vakkennis is een belangrijke oorzaak van de moeilijk vervulbare vacatures. Het aandeel werkgevers in de ICT-dienstverlening dat problemen ervaart door een gebrek aan personeel (40%) is duidelijk groter dan gemiddeld (24%) (p. 2). Bovendien blijkt uit het Factsheet dat het tekort vooral geldt voor ICT'ers met een diploma op hbo/wetenschappelijk niveau en specifiek voor functies als bijvoorbeeld securityspecialisten. Van de moeilijk vervulbare functies is 78% op hbo-niveau (p. 2). Aanvrager stelt dat een forse groei van de vraag naar security specialisten wordt voorzien. De toegenomen digitalisering en de sterke vraag naar gegevensbeveiliging heeft er volgens aanvrager voor gezorgd dat de werkgelegenheidsgroei onder de nog relatief bescheiden groep security specialisten het grootst was van alle ICT-beroepen (+54%, p. 5).

Aanvrager verwijst daarnaast naar het Factsheet 'Arbeidsmarkt Financiële dienstverlening' van het UWV waarin wordt gesteld dat de ICT functionaliteit bij financiële dienstverleners steeds belangrijker wordt. Aanvrager constateert dat in deze sector een tekort aan ict'ers bestaat. Het belang van cybersecurity neemt toe en ook de vraag naar datascientists of BI-specialisten (p. 7). Deze moeilijk vervulbare functies doen zich volgens aanvrager voor op hoger en wetenschappelijk niveau. Aanvrager stelt voorts dat uit het Factsheet 'Arbeidsmarkt Overheid' blijkt dat er in de overheidssector behoefte is aan nieuwe ICT professionals. Aanvrager stelt dat er bij de politie specifiek sprake is van tekorten aan cyberexperts. (p. 4). Ook bij defensie is er volgens aanvrager een tekort aan cyberspecialisten op hbo/wo-niveau. De tekorten betreffen specialistische functies zoals ethical hacker, security specialist en informatieanalist.

Het Factsheet 'Arbeidsmarkt Zorg' ten slotte beschrijft hoe het overgrote deel van organisaties in de zorg werkt aan de inzet van nieuwe technologie. Door al deze nieuwe technologieën ontstaan er nieuwe functies. Daardoor zijn er blijkens het Factsheet bijvoorbeeld ICT-medewerkers nodig voor informatieveiligheid (p. 5). De commissie is van mening dat de drie Factsheets blijken geven van een behoefte aan afgestudeerden van de voorgenomen Ad Information Security in de sectoren financiële dienstverlening, overheid en in de zorg.

Aanvrager heeft verder verwezen naar het rapport 'De inventarisatie van acute personeelstekorten en -overschotten' van het UWV (juni 2020) waarin een overzicht wordt gegeven van de arbeidsmarkteffecten van de coronacrisis tot en met juni 2020.

Uit het rapport volgt dat in de ICT vanwege het thuiswerken en gebruik van remote diensten vooral vraag bestond naar professionals met kennis van Cloud-toepassingen, maar ook naar security specialisten om het thuiswerken zo goed en veilig mogelijk te faciliteren. Aanvrager stelt dat deze ook voor de corona-uitbraak moeilijk te vinden waren (p. 14). In het overzicht van 'Kansrijke beroepen' van het UWV (juni 2021) wordt gesteld dat de arbeidsmarkt sinds de uitbraak van het coronavirus drastisch is veranderd. In het rapport wordt de verwachting uitgesproken dat de arbeidsmarkt in de tweede helft van 2021 weer aantrekt (p. 2). Aanvrager stelt dat afgestudeerden van de Ad Information Security in aanmerking komen voor de volgende kansrijke beroepen op hoger en wetenschappelijk beroepsniveau in de sector ICT: BI-specialisten/data-analisten/data scientists, software consultants ERP / CRM, applicatie-, systeem- en functioneel beheerders, datawarehouse ontwikkelaars, database administrators, netwerkbeheerders, specialisten technische infrastructuur en netwerkengineers, architecten ICT, systeemontwikkelaars en security specialisten. De commissie is van mening dat afgestudeerden van de Ad Information Security in aanmerking komen voor een groot deel van de genoemde kansrijke beroepen. Met name het beroep van security specialist is relevant voor afgestudeerden van de voorgenomen opleiding.

Aanvrager doet verder een beroep op het rapport 'Verwachtingen werkgevers voor 2021: indicatie uit werkgeversenquête UWV' van het UWV (april 2021). Aanvrager beschrijft dat het UWV in het najaar van 2020 een enquête heeft gehouden onder ca. 2.800 bedrijfsvestigingen over de verwachtingen voor 2021 ten aanzien van welk nieuw personeel zij nodig denken te hebben en dat mogelijk lastig te vinden is. Aanvrager stelt dat uit het rapport naar voren komt dat in verschillende sectoren behoefte bestaat aan technici en ICT'ers (p. 1) en dat al jaren sprake is van een tekort aan hbo- en wo-opgeleid ICT-personeel (p. 4). Onder andere het beroep consultant ict wordt door werkgevers genoemd als een beroep waarvoor het moeilijk is om personeel te vinden. De commissie is van oordeel dat het rapport 'Verwachtingen werkgevers voor 2021: indicatie uit werkgeversenquête UWV' een indicatie biedt van een behoefte aan afgestudeerden van de Ad Information Security.

De commissie stelt met aanvrager vast dat uit de 'Nationale Beroepengids' (2021) blijkt dat voor de meeste relevante beroepen van de Ad Information Security zoals Cyber Security Specialist, Security Administrator en Systeemontwikkelaar de baankansen zeer goed zijn en voor de beroepen Systeembeheerder, Data protection officer en Medewerker gegevensbeheer goed. Aanvrager verwijst tevens naar de lijst van kansrijke beroepen van Randstad 'Hottest Jobs' (2021). De commissie constateert met aanvrager dat afgestudeerden van de Ad Information Security in aanmerking komen voor het beroep security specialist dat in de top 3 van meest kansrijke beroepen binnen de sector ICT van de lijst 'Hottest Jobs' van Randstad is geplaatst. Een soortgelijk beeld is terug te zien in het rapport 'Emerging Jobs Report the Netherlands' van LinkedIn (2020) en 'Future of Jobs' van het World Economic Forum. De top drie van Emerging Jobs voor Nederland wordt volgens LinkedIn gevormd door data protection officer, growth hacker en privacy officer. In de top 15 staat ook nog de functie Cyber security specialist (nr. 11). Dit functieprofiel sluit volgens aanvrager aan bij dat van een afgestudeerde Ad'er Information Security met het uitstroomprofiel IT Security. Het functieprofiel voor een functionaris gegevensbescherming/data protection officer komt volgens aanvrager grotendeels overeen met die van een afgestudeerde Ad'er Information Security met het uitstroomprofiel Governance & Compliance. Ook in het onderzoek uitgevoerd door World Economic Forum komt naar mening van aanvrager naar voren dat Information Security Analysts een opkomend beroep is (p. 30). Het beroep staat op de 8e plek in de top 20 met opkomende beroepen over alle sectoren en voor Nederland specifiek op de 8e plek in de top 10 opkomende beroepen (p. 93). De commissie is van mening dat de genoemde opkomende beroepen een indicatie bieden van een behoefte aan afgestudeerden van de Ad Information Security.

Aanvrager beschrijft dat uit het 'Trendrapport ICT en Creatieve Industrie' van de SBB (2020) volgt wat de belangrijkste ontwikkelingen zijn voor de sector ICT en Creatieve industrie en welke ontwikkelingen er binnen het beroepsonderwijs geanticipeerd moeten worden (zie <https://trendrapport.s-bb.nl/ictci/samenvatting-ict/>). Het rapport maakt volgens aanvrager duidelijk dat de digitalisering alle sectoren onder druk zet en de behoefte aan ICT-specialisten in alle sectoren groeit. Cyberveiligheid zal daarbij een steeds belangrijkere rol gaan spelen. Kennis van wet- en regelgeving, veilige software kunnen ontwikkelen, kunnen hacken van systemen en het goed kunnen inzetten van hardware en software binnen een organisatie worden daarom belangrijke benodigde vaardigheden als gevolg van cyberveiligheid. Aanvrager is van mening dat afgestudeerden van de Ad Information Security over deze kennis en vaardigheden beschikken. De commissie is van oordeel dat het 'Trendrapport ICT en Creatieve Industrie' blijk geeft van een kwalitatieve behoefte aan afgestudeerden van de voorgenomen opleiding.

Aanvrager verwijst daarnaast naar het 'Nationaal Techniekpact'. Het doel van het 'Nationaal Techniekpact' is het verbeteren van de aansluiting van het onderwijs op de arbeidsmarkt in de technieksector en daarmee het tekort aan technisch personeel terugdringen. Volgens de Techniekpactmonitor is het lastig om ICT-personeel te vinden, ook in andere sectoren dan de ICT-sector. Door de toename van het thuiswerken is er volgens aanvrager bovendien extra vraag naar professionals met kennis van Cloud toepassingen en security specialisten. Aanvrager beschrijft dat tussen 2016 en 2019 een stijgende trend viel waar te nemen wat betreft openstaande vacatures voor ICT beroepen. In het eerste kwartaal van 2020 is door Covid-19 een trendbreuk te zien in de stijging, waarna in het eerste kwartaal van 2021 het aantal openstaande vacatures weer sterk stijgt. De stijging deed zich vooral voor op beroepsniveau 3 en 4. Voor een opleiding op Ad-niveau is beroepsniveau 3 volgens aanvrager relevant. Het aantal openstaande vacatures op dit niveau steeg van 2.000 in 2016 tot 3.700 in het tweede kwartaal van 2021. Specifiek voor het landsdeel Zuidwest ging het om een stijging van 500 tot 900 openstaande vacatures op beroepsniveau 3 in dezelfde periode. De commissie constateert dat uit het 'Nationaal Techniekpact' volgt dat het aantal vacatures voor ICT beroepen op het relevante beroepsniveau 3 in de afgelopen jaren is gestegen en dat dit een indicatie biedt van een behoefte aan afgestudeerden van de Ad Information Security.

Aanvrager verwijst verder naar een aantal bronnen met betrekking tot digitalisering binnen het mkb. Digitalisering is binnen het mkb een kernelement om concurrerend te blijven en toekomstbestendig te zijn ('Digitalisering in het mkb' van de Kamer van Koophandel, 2019). Uit de 'Cybersecurity Health Check' (2019) die Baker Tilly heeft uitgevoerd onder bijna 200 kleine en middelgrote Nederlandse organisaties blijkt dat de digitale weerbaarheid van deze organisaties nog niet op niveau is. Er moeten volgens het rapport stappen worden gemaakt in het tijdig detecteren van zwaktes in de eigen beveiliging en in het voorbereiden op hoe te reageren bij een cyberincident (p. 1). Ook in het 'Cybersecuritybeeld Nederland 2021' van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV, 2021) komt dit beeld naar voren (p. 10). Aanvrager stelt verder dat mkb-bedrijven aan de slag moeten met de Algemene verordening gegevensbescherming (AVG). Ondernemersorganisatie ONL signaleert in het artikel 'Mkb worstelt enorm met de AVG' (2021) dat veel mkb-ondernemers nog worstelen met de AVG en de privacyregelgeving. Ook uit het artikel 'Privacywetgeving AVG, wanneer ben je compliant?' van de KvK (2019) blijkt dat de meeste Nederlandse bedrijven drie jaar na invoering nog altijd niet voldoen aan de AVG. Aanvrager betoogt dat hieruit volgt dat er specifiek bij mkb-bedrijven een grote behoefte is aan professionals met security kennis. De voorgenomen opleiding heeft als specifiek doel om op te leiden voor het mkb in de regio Rijnmond. De commissie is van mening dat afgestudeerden van de Ad Information Security beschikken over de kennis en vaardigheden op het gebied van cyberveiligheid en privacybescherming waar op dit moment behoefte aan is binnen mkb-bedrijven.

Onder verwijzing naar het onderzoek 'Cybersecurity Talent: the Big Gap in Cyber Protection' van het Digital Transformation Institute van Capgemini (2018) stelt aanvrager dat er weinig aanbod en veel vraag naar professionals met cybersecurityvaardigheden is. In het onderzoek zijn meer dan 1.200 senior executives en eerstelijnsmedewerkers ondervraagd vanuit negen landen waaronder Nederland. Van alle digitale vaardigheden bestaat op het gebied van cybersecurity vaardigheden de grootste kloof tussen de verwachte vraag en het aanbod bij medewerkers (p. 4). Verwacht wordt dat de vraag naar dit soort kennis ook niet gaat afnemen in de komende jaren (gerekend vanaf 2018). De commissie is met aanvrager van mening dat de Ad Information Security een praktijkgericht programma op het gebied van cybersecurity aanbiedt en dat de resultaten van voornoemd onderzoek blijk geven van een arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen opleiding.

Aanvrager verwijst voor wat betreft de regionale arbeidsmarktbehoefte naar het rapport 'Regio in Beeld Rijnmond' van het UWV (2021) en constateert dat de werkgelegenheid voor de sector ICT in 2020, ondanks de coronacrisis, is toegenomen. De beroepsklasse ICT is voor de regio Rijnmond getypeerd als zeer krap en de krapste beroepsklasse in de regio (p. 21). Voor de regio Rijnmond zijn in de sector ICT negen beroepen met moeilijk vervulbare vacatures (zie 'Moeilijk vervulbare vacatures: regionaal overzicht' van het UWV, 2019, p. 47), waaronder de beroepen Security specialisten, Adviseurs interne controle en beveiliging informatievoorziening. Daarnaast wordt in het regionale overzicht 'Kansrijke beroepen. Rijnmond' van het UWV (2021) voor de regio Rijnmond het beroep Security specialist als kansrijk beroep voor de sector ICT genoemd. De commissie is van mening dat het rapport 'Regio in Beeld Rijnmond' aangevuld met het overzicht van moeilijk vervulbare vacatures en kansrijke beroepen blijk geeft van een regionale arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen Ad Information Security.

Aanvrager beschrijft dat in de 'Economische Verkenning Rotterdam' van 2020 wordt gesteld dat Rotterdam al geruime tijd een aanzienlijk aantal banen telt in de creatieve industrie en de ICT-sector. De ICT en creatieve industrie laten sinds enkele jaren een forse groei zien en dragen volgens aanvrager substantieel bij aan de economische voorspoed in Rotterdam (p. 22). In Rotterdam was het aantal banen in de ICT tussen 2015 en 2018 met 13,1% gegroeid met 6.820 banen, t.o.v. een groei van bijvoorbeeld 7,2% in Amsterdam (p. 23). De verwachting is op basis van de 'Economische Verkenning' dat de groei van banen in de ICT-sector doorzet voor de regio. De krapte is volgens de 'Economische Verkenning Rotterdam' het grootst bij ICT-beroepen voor het hoger en wetenschappelijk beroepsniveau (p. 30). Voor hoger opgeleiden is in Rotterdam ICT de belangrijkste sector en de vraag naar IT-professionals is in elke sector groot (p. 30). De meest recente 'Economische Verkenning Rotterdam' (2021) gaat vooral in op de effecten van Covid-19 op de regionale arbeidsmarkt. Hierin wordt gesteld dat de ICT sector de laatste jaren snel groeide in Rotterdam en dat de coronacrisis juist positief uit heeft gepakt voor deze sector (p. 8). De commissie constateert dat uit de 'Economische Verkenning Rotterdam' van 2020 en 2021 volgt dat het aantal banen in de ICT in de regio Rotterdam blijft groeien en dat sprake is van een zeer krappe arbeidsmarkt. De commissie concludeert dan ook dat deze bronnen een indicatie bieden van een arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen opleiding.

Aanvrager beschrijft verder dat op 'Rijnmondinzicht.nl' (2021), het arbeidsmarktdashboard voor de regio Rijnmond, inzicht wordt gegeven in de ontwikkeling van vraag en aanbod op de arbeidsmarkt in de regio. Aanvrager constateert dat er enkele voor de Ad Information Security relevante beroepen in de top drie staan. Het gaat om software- en applicatieontwikkelaars (meeste vacatures in zowel 2019 als 2020) en om databank- en netwerkspecialisten (derde meeste vacatures in zowel 2019 als 2020). Het dashboard 'Zuid-Holland Inzicht' (2021) laat een grote toename in het aantal online vacatures op hbo-/wo-niveau voor de beroepsgroep Software- en applicatieontwikkelaars zien. In mei 2021 waren er 1.101 online openstaande vacatures op dit niveau. Op mbo-niveau-3/4 waren er in dezelfde maand 7 online vacatures. Voor de beroepsgroep Databank- en netwerkspecialisten is een soortgelijke ontwikkeling in de provincie Zuid-Holland waar te nemen, met in mei 2021 562 online vacatures op hbo-/wo-niveau en 18 online vacatures

op mbo-niveau-3/4 voor deze beroepsgroep. De commissie is van mening dat met name de beroepsgroep Databank- en netwerkspecialisten relevant is voor de Ad Information Security. Het aantal beschikbare online vacatures voor deze beroepsgroep geeft volgens de commissie blijk van een arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen Ad.

Aanvrager heeft onderzoeksbureau Lexnova gevraagd om een kwantitatief arbeidsmarktonderzoek uit te voeren om de behoefte aan afgestudeerden van de Ad Information Security te peilen. Het onderzoek is in het najaar van 2021 uitgevoerd onder 72 werkgevers van verschillende organisaties in de provincies Zuid-Holland en Zeeland. De respons is via twee bronnen verzameld: een adressenbureau en het netwerk van Hogeschool Rotterdam. Na het samenvoegen van de respons vanuit deze twee databronnen is er gecontroleerd op dubbele organisaties. Op deze manier is volgens Lexnova gewaarborgd dat er per organisatie één respondent deelgenomen heeft. Niet alle respondenten hebben alle vragen beantwoord. Er is per vraag aangegeven wat de respons is (de n). Alle werkgevers hebben een leidinggevende functie en/of zijn (mede)verantwoordelijk voor het aannemen en/of bijscholen van medewerkers. Bijna driekwart van de respondenten is werkzaam binnen het mkb. De vragenlijst alsmede de antwoorden op de open vragen zijn als bijlage toegevoegd. Lexnova heeft noch de namen van de respondenten noch de organisaties waarvoor zij werkzaam zijn bekendgemaakt. De commissie acht de uitkomsten van het onderzoek om die reden niet volledig navolgbaar.

In de enquête is het profiel van de Ad Information Security voorgelegd. 92% van de potentiële werkgevers acht de inhoud en de opzet van de Ad-opleiding (zeer) aansprekend. De behoefte in het werkveld aan medewerkers die de Ad Information Security hebben gevolgd geeft volgens aanvrager eveneens een positief beeld: 66% is het (helemaal) eens met de stelling dat er in het werkveld behoefte is aan deze medewerkers. Hierna is gevraagd of de werkgevers nieuwe medewerkers met een afgeronde Ad Information Security binnen hun eigen organisatie zouden aannemen. In absolute aantallen is door 13 van de 72 werkgevers (18%) aangegeven dat zij in de komende drie jaar zeker behoefte hebben aan nieuwe medewerkers met een Ad Information Security. Voor 31 van de 72 werkgevers geldt dat zij hier mogelijk behoefte aan hebben (43%). Werkgevers die zeker behoefte hebben geven aan in totaal minimaal 68 en maximaal 158 medewerkers nodig te hebben in de komende drie jaar. De jaarlijkse behoefte van deze werkgevers komt daarmee volgens aanvrager uit op minimaal 23 en maximaal 53 medewerkers met een afgeronde Ad Information Security. Ook is er behoefte aan bij-, om- of opscholing van huidige medewerkers met de Ad Information Security. In absolute aantallen is door 9 van de 72 werkgevers (13%) aangegeven dat zij zeker behoefte hebben aan het bij-, om- of opscholen van hun huidige medewerkers met een Ad Information Security. Voor 31 van de 72 (43%) geldt dat zij hier mogelijk behoefte aan hebben. Gezamenlijk geven deze werkgevers aan behoefte te hebben aan bij-, om- of opscholing van in totaal minimaal 217 en maximaal 420 medewerkers. De werkgevers die zeker behoefte hebben geven aan dat dit per jaar om in totaal minimaal 38 en maximaal 78 medewerkers gaat. De commissie concludeert dat uit het onderzoek weliswaar een arbeidsmarkt- en opscholingsbehoefte naar voren komt, maar dat het onderzoek vanwege het ontbreken van de namen van de respondenten en de organisaties waar zij werkzaam zijn slechts ten dele navolgbaar is. De commissie is dan ook terughoudend om veel gewicht aan de resultaten van het onderzoek toe te kennen.

Ten slotte heeft aanvrager Lexnova opdracht gegeven om kwalitatief onderzoek te verrichten door middel van het afnemen van interviews bij twaalf organisaties in de regio (september 2021). De geïnterviewde personen zijn werkzaam bij verschillende organisaties in de ICT, overheden, zorg en zakelijke dienstverlening en zijn allen betrokken bij werving en selectie van professionals op het gebied van informatiebeveiliging. Een overzicht van de geïnterviewden (functie en organisatie waar zij werkzaam zijn), de gespreksleidraad en de gespreksverslagen zijn als bijlage toegevoegd. De commissie acht het kwalitatieve onderzoek valide en navolgbaar. Aanvrager geeft aan dat de geïnterviewde werkgevers positief zijn over het opleidingsprofiel van de Ad Information Security

en dat de inhoud en de opzet van de Ad goed aansluiten bij de ontwikkelingen in de sector en de wensen van het werkveld. Uit de interviews blijkt volgens aanvrager dat de respondenten van mening zijn dat er op dit moment nog geen opleiding is die op dezelfde manier governance met cybersecurity verbindt. Uit de interviews komt volgens aanvrager een zeer positief beeld naar voren van de arbeidsmarktperspectieven voor afgestudeerden van de Ad Information Security. Werkgevers zien in diverse type organisaties en sectoren behoefte ontstaan aan afgestudeerden van de voorgenomen Ad: binnen ICT organisaties, maar ook binnen het mkb, de zorg, overheden en het onderwijs. Er wordt aangegeven dat er momenteel krapte bestaat en dat er verwacht wordt dat deze vraag blijft of zelfs groter wordt. Zeven van de twaalf geïnterviewde werkgevers geeft aan binnen hun eigen organisatie binnen 2 tot 5 jaar nieuwe medewerkers aan te willen nemen met een Ad Information Security. De inschattingen variëren van 2 tot 6 medewerkers, waarbij de meeste werkgevers aangeven 3 tot 5 aan te willen nemen. Wanneer het gaat over het op- of bijscholen van huidige medewerkers met de Ad Information Security geven vier van de twaalf werkgevers aan hier interesse in te hebben. Eén werkgever geeft aan dat dit momenteel niet geval is maar denkt hier in de toekomst behoefte aan te hebben. De commissie is van mening dat uit de interviews een arbeidsmarktbehoefte aan c.q. opscholingsbehoefte van afgestudeerden van de Ad Information Security naar voren komt.

De commissie concludeert op grond van het bovenstaande dat aanvrager een grote arbeidsmarktbehoefte aan afgestudeerden van de Ad Information Security heeft aangetoond. Aanvrager heeft tevens aangetoond dat de voorgenomen Ad kan voorzien in een opscholingsbehoefte.

Beoordeling maatschappelijke behoefte

Aanvrager verwijst ter onderbouwing van de maatschappelijke behoefte onder meer naar 'Houdbaar voor de toekomst. Strategische agenda hoger onderwijs en onderzoek' van het Ministerie van Onderwijs, Cultuur en Wetenschap (2019), 'Professionals voor Morgen. Strategische agenda 2019-2023' van de Vereniging Hogescholen (2019), de 'Nederlandse Cybersecurity Agenda' afkomstig van het Nationaal Cyber Security Centrum van het Ministerie van Justitie en Veiligheid (2018) en de Kamerbrief 'Voortgang Nederlandse Cybersecurity Agenda' van de toenmalige minister van Justitie en Veiligheid (2019), het artikel 'Beschermen van een veilig digitaal Nederland' (via: <https://www.nctv.nl/themas/cybersecurity>) van de Nationaal Coördinator Terrorismebestrijding en Veiligheid/NCTV (2021), het rapport 'Cybersecuritybeeld Nederland 2021' van de NCTV (2021) en het rapport 'Integrale aanpak cyberweerbaarheid' van de Cyber Security Raad (2021).

Aanvrager beschrijft dat Ad opleidingen voorzien in een vraag op de arbeidsmarkt en de doorstroom van mbo naar hbo versterken. Zowel de 'Strategische Agenda hoger onderwijs en onderzoek' (p. 48) als de 'Strategische Agenda 2019-2023' van de Vereniging Hogescholen (p. 10) onderstrepen het belang van Ad opleidingen en de wens het aanbod van Associate degrees uit te breiden. Aanvrager stelt dat een nieuwe Ad Information Security binnen dit streven past. De commissie is van mening dat uit deze bronnen een algemene behoefte aan Ad opleidingen blijkt.

Aanvrager beschrijft verder dat digitalisering essentieel is geworden om de maatschappij draaiende te houden. De Rijksoverheid zet om die reden in op digitalisering van de economie en onderstreept het toenemende belang van cybersecurity. In de 'Nederlandse Cybersecurity Agenda' (NCSA) worden zeven ambities op het gebied van digitale weerbaarheid genoemd. Deze ambities moeten worden omgezet in concrete maatregelen die cyberdreigingen het hoofd bieden en Nederland digitaal veilig maken.

In de Kamerbrief 'Voortgang Nederlandse Cybersecurity Agenda' (2019) wordt genoemd dat er nog meer concrete acties worden genomen om de digitale slagkracht te vergroten, zoals investeringen in personeel en expertise bij organisaties door middel van werving van meer deskundigen (p. 1). Er wordt een groeiende behoefte aan cybersecurityprofessionals gesignaleerd (p. 5). De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) richt zich op de maatschappelijke opgave om Nederland digitaal vaardig te maken (zie 'Beschermen van een veilig digitaal Nederland' via: <https://www.nctv.nl/themas/cybersecurity>). Het rapport 'Cybersecuritybeeld Nederland 2021' van de NCTV biedt inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast en de weerbaarheid en risico's in Nederland. Volgens het rapport is de weerbaarheid van Nederland tegen cybercrime nog niet voldoende en worden basismaatregelen tegen digitale dreigingen nog te vaak niet of onvoldoende getroffen. Daarnaast concludeert het rapport dat cybercriminelen de nationale veiligheid kunnen raken. In het adviesrapport 'Integrale aanpak cyberweerbaarheid' van de Cyber Security Raad (2021) wordt geconcludeerd dat de digitale veiligheid en autonomie in Nederland onder druk staan. Aanvrager concludeert onder meer uit het rapport dat moet worden ingezet op het opleiden en behouden van professionals met de benodigde digitale vaardigheden (p. 31). De focus zal voornamelijk moeten liggen op het creëren en borgen van hoogwaardig cybersecurity-onderwijs op universiteiten en hogescholen (p. 32). De commissie constateert dat uit al deze stukken blijkt dat de Nederlandse Rijksoverheid sterk inzet op digitalisering van de economie en daarbij ook expliciet aandacht heeft voor digitale veiligheidsvraagstukken. De voorgenomen hbo Ad Information Security sluit daar direct op aan. Reeds op grond hiervan concludeert de commissie dat de opleiding beantwoordt aan een maatschappelijke behoefte.

De commissie concludeert dat de aanvraag aansluit op een maatschappelijke en een arbeidsmarktbehoefte. De aanvraag voldoet aan criterium a in art. 4 lid 1 van de Regeling.

Beoordeling criterium b

Vanaf 11/04/2022 is op de website van de CDHO kennisgegeven van het voornemen van de Hogeschool Rotterdam om de hbo Associate degree Information Security in Rotterdam aan te bieden. Hiermee is aan de instellingen voor hoger onderwijs de mogelijkheid gegeven om hun zienswijzen op dit voornemen kenbaar te maken. Er zijn geen zienswijzen ingediend.

De commissie overweegt ten aanzien van de ruimte in het landelijk opleidingsaanbod als volgt. De commissie beoordeelt de ruimte in het landelijke opleidingsaanbod onder meer door te bepalen welke bestaande opleidingen verwant zijn aan de voorgenomen opleiding. De onderwijsinstelling dient overtuigend te beargumenteren dat er nog voldoende ruimte is voor een nieuwe opleiding. De onderwijsinstelling dient hiertoe aan te geven wat het landelijk verwant aanbod van de aangevraagde opleiding is. Het verwant aanbod is aanbod dat inhoudelijk sterk met elkaar overeenkomt en opleidt tot (min of meer) dezelfde beroepen (uitstroomprofiel(en)). Bij de inhoud wordt door de commissie gekeken of de kennisgebieden en vaardigheden die in het curriculum van de voorgenomen opleiding zijn opgenomen overlap vertonen met de bestaande opleidingen. Voorts kijkt de commissie naar de instroomdoelgroep die de opleiding bedient. Verder is voor de beoordeling van het verwant aanbod van belang om welke onderwijsvariant (voltijd, deeltijd of duaal) het gaat. Verwante opleidingen worden dus niet louter bepaald aan de hand van de inhoud van een opleiding.

Aanvrager heeft de Ad Information Security vergeleken met verwante Associate degrees binnen ROA's opleidingscluster bachelor informatica. Aanvrager is van mening dat de Ad's Cybersecurity (Hogeschool van Amsterdam), IT Security Management (Hogeschool INHOLLAND, aangevraagd en in behandeling bij de CDHO) en Cyber Safety & Security (NHL Stenden Hogeschool, goedgekeurd maar nog niet gestart) het meest verwant aan de Ad Information Security zijn. Daarnaast beschouwt aanvrager de onbekostigde hbo Ad Security Management (LOI) als verwant aan de voorgenomen opleiding.

De commissie deelt de mening van aanvrager dat de hbo Ad's Cybersecurity, IT Security Management en Cyber Safety & Security als verwant aan de voorgenomen opleiding dienen te worden beschouwd. Gezien het feit dat alleen de instroomgegevens van de Ad Cybersecurity bekend zijn is dit de enige sterk verwante opleiding die in het overzicht hieronder is opgenomen (tabel 3). Anders dan aanvrager is de commissie van mening dat de volgende opleidingen als aanverwant dienen te worden beschouwd: de hbo Ad's ICT (Zuyd Hogeschool en Fontys Hogescholen), ICT-Beheer (Christelijke Hogeschool Windesheim en NHL Stenden Hogeschool), Informatica (Avans Hogeschool), ICT Service Management (Hogeschool Rotterdam, Christelijke Hogeschool Ede en Fontys Hogescholen) en IT Service Management (Hogeschool INHOLLAND en NHL Stenden Hogeschool).

Aanvrager heeft een overzicht geleverd van de instroom in verwante bekostigde opleidingen. De instroom in de verwante onbekostigde Ad's Security Management van LOI en de aanverwante onbekostigde hbo Ad's ICT & Telecommunicatie van Hogeschool Dirksen en ICT-Engineer van Da Vinci HBO Drechtsteden is niet bekend. De commissie heeft bij de beoordeling van de aanvraag dan ook geen rekening kunnen houden met de belangen van deze opleidingen.

De instroom in het verwante bekostigde onderwijsaanbod groeide in de afgelopen vijf jaar, met name in het voltijdaanbod (zie tabel 3).

Tabel 3. Instroom in (aan)verwante bekostigde Ad opleidingen

Opleiding	Instelling	'16-'17		'17-'18		'18-'19		'19-'20		'20-'21		'21-'22	
		vt	dt	vt	dt	vt	dt	vt	dt	vt	dt	vt	dt
Ad Cybersecurity (80156)	Hogeschool van Amsterdam (28DN), Amsterdam							53		81		86	
Ad AD-ICT (80152)	Fontys Hogescholen (30GB), Eindhoven									27	27	44	62
	Fontys Hogescholen (30GB), Tilburg							21		55		48	
Ad ICT (80132)	Zuyd Hogeschool (25JX), Heerlen			100	10	92		54		88		67	2
Ad ICT Service Management (80083)	Christelijke Hogeschool Ede (25BA), Ede							11		9		9	6
	Fontys Hogescholen (30GB), Eindhoven			31		20		26		20		3	2
	Hogeschool Rotterdam (22OJ), Rotterdam	61	17	77	41	68	28	50	26	45	25	30	27
Ad ICT-Beheer (80071)	NHL Stenden Hogeschool (31FR), Emmen	12		10		8		5		13		13	
Ad Informatica (80075)	Avans Hogeschool (07GR), Breda									25		39	22
	Avans Hogeschool (07GR), Roosendaal					27		25		28		25	
Ad IT Service Management (80024)	Hogeschool INHOLLAND (27PZ), Diemen			15		15		16	20	30	10	23	8
	NHL Stenden Hogeschool (31FR), Leeuwarden	6		5		4		7	6	10	6	15	12
Eerstejaarsinstroom	Totaal	79	48	207	71	214	65	231	106	377	119	351	141

Bron: DUO

Aanvrager heeft een prognose gemaakt van de instroom in de voorgenomen opleiding op grond van een instroomonderzoek van Lexnova (2021) dat is uitgevoerd onder 122 studenten van verwante mbo-4-opleidingen en 42 havisten van middelbare scholen in de regio Rotterdam. Aanvrager verwacht dat in de voltijdvariant in de eerste jaren 15-20 studenten per jaar zullen instromen oplopend tot ruim 40 studenten op jaarbasis. Voor de deeltijdvariant van de Ad Information Security is de verwachting dat er gestart zal worden met een klas van 25-30 studenten per jaar oplopend tot ruim 60 studenten per jaar. De commissie acht deze prognoses in ieder geval voor de eerste jaren realistisch.

Als de instroom in de bestaande opleidingen en de verwachte instroom in de voorgenomen hbo Associate degree Information Security wordt afgezet tegen de behoefte die bij criterium a is aangetoond, blijkt dat er voldoende ruimte is om deze opleiding binnen het bekostigde domein vorm te geven.

Vestiging van de opleiding in Rotterdam heeft geen negatief effect op de landelijke spreiding van het onderwijsaanbod, aangezien er slechts 1 aanverwante Ad opleiding in Rotterdam is gevestigd (ICT Service Management).

De commissie concludeert dat er ruimte in het landelijk aanbod bestaat om de hbo Associate degree Information Security te realiseren. De aanvraag voldoet aan criterium b in art. 4 lid 1 van de Regeling.

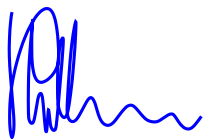
Gelet op het vorenstaande adviseert de Commissie Doelmatigheid Hoger Onderwijs u om positief te besluiten op het voorliggende verzoek.

Advies aan de NVAO over de naamkeuze en Croho indeling

De commissie merkt op dat hierboven is geconstateerd dat de voorgenomen hbo Associate degree Information Security sterke verwantschap vertoont met een aantal bestaande opleidingen. Omwille van de transparantie van het opleidingsaanbod adviseert de commissie om de naam van de voorgenomen opleiding aan te laten sluiten bij de reeds geregistreerde opleidingsnaam Cybersecurity. Bovendien heeft de commissie geconstateerd dat aanvrager de hbo Associate degree Information Security in het Croho onderdeel Techniek wil indelen. Dit voorstel sluit aan op de indeling van verwante bestaande opleidingen.

De NVAO ontvangt dit advies, zodat zij dit kan opnemen in het informatiedossier voor het panel ten behoeve van de toets nieuwe opleiding.

De Commissie Doelmatigheid Hoger Onderwijs



drs. P.M.M. Rullmann

Voorzitter CDHO

Bijlage:

Beoordelingskader macrodoelmatigheid nieuwe opleiding of nevenvestiging

Aan de hand van de in de Regeling macrodoelmatigheid hoger onderwijs van 20 juni 2018 genoemde voorwaarden worden voornemens tot het verzorgen van een nieuwe opleiding beoordeeld op doelmatigheid. Een nieuwe opleiding kan volgens artikel 4 van deze Regeling alleen doelmatig worden geacht indien het voornemen voldoet aan de criteria a en b.

Volgens criterium a heeft het instellingsbestuur aangetoond dat er behoefte bestaat aan de nieuwe opleiding of nevenvestiging, zijnde overwegend een arbeidsmarktbehoefte, dan wel een overwegend maatschappelijke behoefte in combinatie met een arbeidsmarktbehoefte, dan wel een overwegend wetenschappelijke behoefte in combinatie met een arbeidsmarktbehoefte.

Volgens criterium b dient het instellingsbestuur aan te tonen dat in de behoefte die bij criterium a is aangetoond niet door het bestaande opleidingsaanbod wordt voorzien.

Advies aan de NVAO over naamkeuze en Croho onderdeel

In de Toelichting op de Regeling is aangegeven dat de CDHO ook een rol heeft bij de beoordeling van de voorgestelde naam en voertaal van de opleiding en bij de voorgestelde positionering in het Croho.

Wat betreft de opleidingsnaam: de CDHO kijkt of de voorgestelde naam van de opleiding passend is, gelet op de namen van verwante opleidingen. Daarbij is het uitgangspunt dat sterk op elkaar lijkende opleidingen dezelfde naam krijgen, om de transparantie van het opleidingsaanbod voor studiekezers en werkgevers te borgen. In het Croho kan ook een internationale (Engelse) naam worden geregistreerd. Dit onderdeel van het CDHO advies is niet gericht aan de Minister van OCW, maar aan de NVAO. Het panel van de NVAO toetst of de naamkeuze gerechtvaardigd is gelet op de inhoud van de opleiding en de namen van vergelijkbare opleidingen (artikel 5.7, vierde lid, onderdeel a, van de WHW).

Wat betreft de positie in het Croho: de CDHO kijkt of de voorgestelde indeling in het Croho passend is, gelet op de indeling van verwante opleidingen. Daarbij is het uitgangspunt dat sterk op elkaar lijkende opleidingen in hetzelfde Croho onderdeel worden geregistreerd, om de transparantie van het opleidingsaanbod voor studiekezers en werkgevers te borgen. Dit onderdeel van het CDHO advies is niet gericht aan de Minister van OCW, maar aan de NVAO. Het panel van de NVAO toetst of de voorgestelde indeling in het Croho aansluit bij de ordening van verwante opleidingen.