Ministerie van Onderwijs, Cultuur en Wetenschap

Ontvangen: 27-2-2023 2022/094++vt

>Retouradres Postbus 16375 2500 BJ Den Haag

Hogeschool Utrecht
T.a.v. het College van Bestuur
Postbus 573
3500 AN UTRECHT

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

Onze referentie
35561577

Bijlagen
1

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.

Datum 27 februari 2023
Betreft Besluit macrodoelmatigheid hbo-masteropleiding Digitale Veiligheid

Geacht college,

Met de brief van 6 december 2022, door de Commissie Doelmatigheid Hoger Onderwijs (hierna: CDHO) ontvangen op 8 december 2022, hebt u mij het voornemen voorgelegd om de hbo-masteropleiding Digitale Veiligheid als bekostigde opleiding te verzorgen in Utrecht.

Advies CDHO
De CDHO heeft mij bij brief van 16 januari 2023, kenmerk 2022/094, positief geadviseerd over uw aanvraag. Dit advies, dat integraal deel uitmaakt van dit besluit, treft u hierbij aan.

Besluit
Gelet op het bovengenoemd advies 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 hbo-masteropleiding Digitale Veiligheid als bekostigde opleiding te verzorgen in Utrecht. Met toepassing van artikel 6.2, derde lid, van de WHW, beperk ik mijn instemming tot de voltijdvariant.

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 dit besluit is geregistreerd in het Croho. Registratie binnen die termijn is niet eerder mogelijk dan nadat de NVAO 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 bij de NVAO een aanvraag voor de toets nieuwe opleiding in te dienen. 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.

Een afschrift van deze brief is verzonden aan de CDHO, de NVAO, DUO-Groningen, de Inspectie van het Onderwijs en de VH.

Met vriendelijke groet,

de minister van Onderwijs, Cultuur en Wetenschap,
namens deze,
de directeur Hoger Onderwijs en Studiefinanciering,

Commissie Doelmatigheid Hoger Onderwijs

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

Begeleidend schrijven bij advies

Onderwerp	*Ons Kenmerk*	*Datum*
Nieuwe opleiding Hogeschool Utrecht Voltijd hbo master Digitale Veiligheid Utrecht	2022/094	16/01/2023

Geachte heer Dijkgraaf,

Hierbij ontvangt u het advies van de CDHO over de aanvraag van de Hogeschool Utrecht voor de nieuwe hbo master Digitale Veiligheid te Utrecht. De commissie adviseert de toestemming te beperken tot de voltijdvariant op grond van art. 6.2 lid 3 WHW.

Een afschrift van uw besluit zie ik graag tegemoet.

Met vriendelijke groet,

drs. P.M.M. Rullmann
Voorzitter CDHO

Bijlage:
advies CDHO

Commissie Doelmatigheid Hoger Onderwijs

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 Utrecht Voltijd hbo master Digitale Veiligheid Utrecht	2022/094	16/01/2023

Geachte heer Dijkgraaf,

Op 08/12/2022 heeft de Commissie Doelmatigheid Hoger Onderwijs het voornemen ontvangen van de Hogeschool Utrecht om de hbo master Digitale Veiligheid als bekostigde opleiding te verzorgen te Utrecht (brief van 06/12/2022 met kenmerk 2022/MasterDV/MS/MD/061222). 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 Utrecht om de hbo master Digitale Veiligheid als bekostigde opleiding te Utrecht te verzorgen. De commissie adviseert daarbij de toestemming te beperken tot de voltijdvariant op grond van art. 6.2 lid 3 van de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW).

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
De aanvrager wil de opleiding Digitale Veiligheid in Utrecht vestigen. Het gaat om een Nederlandstalige hbo master die de aanvrager in het Croho onderdeel Gedrag en Maatschappij wil laten registreren. De voorgenomen opleiding omvat 60 studiepunten en de aanvrager wil deze in voltijdvorm aanbieden.

De opleiding is inhoudelijk gericht op de digitale weerbaarheid van de samenleving en de manier waarop deze op de lange termijn kan worden gewaarborgd. Afgestudeerden leren risico's verbonden aan het digitale domein en de rol van digitalisering voor de continuïteit en ontwikkeling van organisaties te herkennen. Het programma besteedt naast de technologische en organisatorische zijde van informatiebeveiliging ook aandacht aan wet- en regelgeving, ethiek, sociale psychologie en verandermanagement.
De opleiding is toegankelijk voor alle studenten met een afgeronde bacheloropleiding Integrale Veiligheid, HBO-Recht of ICT.
Afgestudeerden van de opleiding kunnen onder meer de functies (information) security officer, privacy officer, functionaris gegevensbescherming en security architect uitvoeren.

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
De aanvrager stelt dat de hbo master Digitale Veiligheid aansluit op een arbeidsmarktbehoefte in combinatie met een maatschappelijke behoefte.

Beoordeling arbeidsmarktbehoefte
Ter onderbouwing van de arbeidsmarktbehoefte beroept de aanvrager zich op de prognoses voor opleidingstypen en beroepsgroepen zoals deze zijn opgenomen in het AIS van het ROA, het rapport 'European Cybersecurity Skills Framework' van het European Union Agency for Cybersecurity (2022), een interview met Raymond Slot, lector Cyber Security bij de aanvrager (2022), de 'Nederlandse Cybersecuritystrategie 2022-2028' (2022), het 'Opschalingsplan Human Capital Agenda ICT: Regionale initiatieven voor om- en bijscholing digitalisering 2021 – 2025' van de Human Capital Agenda ICT (2021), de 'Nederlandse Digitaliseringsstrategie 2021' van de Rijksoverheid (2021), de website van NationaleBeroepengids.nl (www.nationaleberoepengids.nl/information-security-manager), de Spanningsindicator van het UWV (www.werk.nl/arbeidsmarktinformatie/dashboards/spanningsindicator), het rapport 'Kansrijke beroepen' van het UWV (2021), het rapport 'ICT-beroepen: Barometer arbeidsmarkt' van het UWV (2021), het factsheet 'Overheid: Factsheet arbeidsmarkt' van het UWV (2020), het rapport 'Moeilijk vervulbare vacatures en behoud van personeel: ervaringen werkgevers' van het UWV (2022), het rapport 'Moeilijk vervulbare vacatures: Landelijk overzicht van beroepen' van het UWV (2019) en het arbeidsmarktonderzoek 'Marktpotentieel Master Digitale Veiligheid: Hogeschool Utrecht' dat in opdracht van de aanvrager is uitgevoerd door Lexnova (2022).
De commissie laat het interview met Raymond Slot, lector Cyber Security bij de aanvrager (2022) buiten beschouwing omdat de geïnterviewde partij werkzaam is bij de aanvrager en als zodanig niet als een onafhankelijke bron kan worden gezien.

De aanvrager beschouwt twee opleidingstypen die zijn opgenomen in het AIS van het ROA als relevant voor de voorgenomen opleiding Digitale Veiligheid, zijnde het opleidingstype master management, bedrijfs- en personeelswetenschappen en het opleidingstype master informatica. De commissie neemt het opleidingstype master informatica niet mee bij de beoordeling van de arbeidsmarktbehoefte omdat hier geen verwante opleidingen in zijn opgenomen.

De commissie acht met de aanvrager het opleidingstype master management, bedrijfs- en personeelswetenschappen ten dele relevant omdat de aanverwante opleiding Interdisciplinary Business Professional hierin is opgenomen, samen met enkele opleidingen met aanverwante tracks en een groot aantal niet en nauwelijks verwante opleidingen. ROA typeert de vooruitzichten in 2026 voor afgestudeerden van dit opleidingstype als goed en verwacht grote knelpunten in de toekomstige personeelsvoorziening (zie Tabel 1).

Tabel 1. Arbeidsmarktprognoses opleidingstype master management, bedrijfs- en personeelwetenschappen

Opleidingstype	Arbeidsmarktprognose variabele	Indicator	Aantal	Totaal % 6 jr.	Gem. jaarlijks %	Typering
> > Master - management, bedrijfs- en personeelwetenschappen	verwachte uitbreidingsvraag tot 2026		19600	9	1.4	hoog
> > Master - management, bedrijfs- en personeelwetenschappen	verwachte vervangingsvraag tot 2026		30200	13	2.1	gemiddeld
> > Master - management, bedrijfs- en personeelwetenschappen	verwachte baanopeningen tot 2026		49800	22	3.3	gemiddeld
> > Master - management, bedrijfs- en personeelwetenschappen	verwachte instroom van schoolverlaters tot 2026		44100	19	3	gemiddeld
> > Master - management, bedrijfs- en personeelwetenschappen	ITKP toekomstige knelpunten personeelsvoorziening in 2026	1				groot
> > Master - management, bedrijfs- en personeelwetenschappen	ITA toekomstige arbeidsmarktsituatie in 2026	1				goed

Bron: ROA, AIS

De aanvrager beroept zich tevens op de prognoses van het ROA voor de beroepsgroepen bedrijfskundigen en organisatieadviseurs, beleidsadviseurs en managers ICT. De commissie kent in beginsel meer gewicht toe aan de prognoses voor opleidingstypen omdat daarin de uitstroom uit een cluster verwante opleidingen wordt gerelateerd aan verwachte baanopeningen voor dit type afgestudeerden.

De commissie acht met de aanvrager de beroepsgroep bedrijfskundigen en organisatieadviseurs relevant omdat afgestudeerden van de voorgenomen opleiding in aanmerking komen voor een deel van de beroepen binnen deze beroepsgroep, zoals bedrijfskundigen en organisatieadviseurs. Uit de prognose van het ROA blijkt dat er voor deze beroepsgroep grote knelpunten in de toekomstige personeelsvoorziening worden verwacht (zie Tabel 2).

Tabel 2. Arbeidsmarktprognoses beroepsgroep bedrijfskundigen en organisatieadviseurs

Beroepsgroep	Arbeidsmarktprognose variabele	Indicator	Aantal	Totaal % 6 jr.	Gem. jaarlijks %	Typering
Bedrijfskundigen en organisatieadviseurs	verwachte uitbreidingsvraag tot 2026		14600	11	1.7	erg hoog
Bedrijfskundigen en organisatieadviseurs	verwachte vervangingsvraag tot 2026		14100	10	1.7	laag
Bedrijfskundigen en organisatieadviseurs	verwachte baanopeningen tot 2026		28700	21	3.3	gemiddeld
Bedrijfskundigen en organisatieadviseurs	ITKB toekomstige knelpunten beroepsgroep in 2026	0.831				groot

Bron: ROA, AIS

Daarnaast acht de commissie met de aanvrager de beroepsgroep managers ICT ten dele relevant omdat afgestudeerden van de voorgenomen opleiding in aanmerking komen voor een deel van de beroepen managers informatie- en communicatietechnologie die hierin zijn opgenomen. De commissie stelt hierbij wel dat afgestudeerden enkel in aanmerking zullen komen voor beroepen waarbij geen diepgaande kennis van ICT nodig is. Uit de prognose van het ROA blijkt dat er voor deze beroepsgroep grote knelpunten in de toekomstige personeelsvoorziening worden verwacht (zie Tabel 3).

Tabel 3. Arbeidsmarktprognoses beroepsgroep managers ICT

Beroepsgroep	Arbeidsmarktprognose variabele	Indicator	Aantal	Totaal % 6 jr.	Gem. jaarlijks %	Typering
Managers ICT	verwachte uitbreidingsvraag tot 2026		1700	7	1.2	gemiddeld
Managers ICT	verwachte vervangingsvraag tot 2026		3000	13	2.1	gemiddeld
Managers ICT	verwachte baanopeningen tot 2026		4700	21	3.2	gemiddeld
Managers ICT	ITKB toekomstige knelpunten beroepsgroep in 2026	0.81				groot

Bron: ROA, AIS

Verder acht de commissie de beroepsgroep beleidsadviseurs ten dele relevant omdat afgestudeerden van de voorgenomen opleiding in aanmerking komen voor een deel van de beroepen binnen deze beroepsgroep. De commissie acht deze groep ten dele relevant omdat zij van mening is dat afgestudeerden vooral in aanmerking zullen komen voor beleidsfuncties waar kennis van digitale vaardigheid bij centraal staat. Uit de prognose van het ROA blijkt dat er voor deze beroepsgroep grote knelpunten in de toekomstige personeelsvoorziening worden verwacht (zie Tabel 4).

Tabel 4. Arbeidsmarktprognoses beroepsgroep beleidsadviseurs

Beroepsgroep	Arbeidsmarktprognose variabele	Indicator	Aantal	Totaal % 6 jr.	Gem. jaarlijks %	Typering
Beleidsadviseurs	verwachte uitbreidingsvraag tot 2026		6900	9	1.4	hoog
Beleidsadviseurs	verwachte vervangingsvraag tot 2026		11300	15	2.3	gemiddeld
Beleidsadviseurs	verwachte baanopeningen tot 2026		18300	24	3.6	gemiddeld
Beleidsadviseurs	ITKB toekomstige knelpunten beroepsgroep in 2026	0.834				groot

Bron: ROA, AIS

De commissie concludeert dat de prognoses die zijn opgenomen in het AIS van het ROA voor de opleidingstypen en beroepsgroepen die (ten dele) relevant zijn voor de onderhavige opleiding een positief beeld geven van de arbeidsmarktperspectieven voor afgestudeerden van de voorgenomen opleiding Digitale Veiligheid.

De aanvrager verwijst verder naar het rapport 'European Cybersecurity Skills Framework' van het European Union Agency for Cybersecurity (2022), waarin de internationale rol van het profiel van afgestudeerden van de voorgenomen opleiding wordt besproken. In dit rapport zijn

functieprofielen gestandaardiseerd voor twaalf rollen, waarvan de volgende drie door de aanvrager als relevant worden beschouwd: (Chief) Information Security Officer, Cyber Legal, Policy & Compliance Officer en Cybersecurity Risk Manager. De aanvrager geeft aan dat de voorgenomen opleiding is ingericht om aan te sluiten op deze functieprofielen. De commissie stelt vast dat de voorgenomen opleiding aansluit op de profielen die in het rapport worden besproken. De commissie constateert dat het feit dat er wordt gewerkt aan een standaardisatie van dit type functieprofielen blijk geven van de professionalisering van dit soort beroepen, wat in de ogen van de commissie een positieve indicatie is van de arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen opleiding.

De aanvrager refereert ook aan de 'Nederlandse Cybersecuritystrategie 2022-2028' (2022, p. 23, 41-44), die op vier pijlers rust. De vierde pijler betreft de 'cybersecurity-arbeidsmarkt, onderwijs en de digitale weerbaarbaarheid van burgers', waarin onder andere het doel is gesteld om aan de toenemende vraag aan cybersecurityexperts op de Nederlandse arbeidsmarkt te kunnen voldoen. Hiervoor stelt de strategie dat er meer opleidingsplekken op alle niveaus (waaronder hbo-niveau) moeten komen. De voorgenomen opleiding sluit aan op deze behoefte.

Het 'Opschalingsplan Human Capital Agenda ICT: Regionale initiatieven voor om- en bijscholing digitalisering 2021 – 2025' van de Human Capital Agenda ICT (2021, p. 2) wordt aangehaald om aan te geven dat de digitalisering steeds meer effect krijgt op de afhandeling van economische en maatschappelijke uitdagingen. De coronacrisis heeft dit verder versneld omdat er steeds meer bedrijven zijn gaan digitaliseren en dat (mede daardoor) de behoefte aan ICT-professionals nu voor bijna 70% buiten de ICT-sector ligt. De Human Capital Agenda ICT heeft het doel gesteld om 36.000 mensen extra op te leiden en/of bij te scholen. De commissie constateert dat deze opleiding in algemene zin aansluit op de behoefte aan meer kennis van het digitale domein op de arbeidsmarkt.

Ook de door de aanvrager aangehaalde 'Nederlandse Digitaliseringsstrategie 2021' van de Rijksoverheid (2021, p. 24) beschrijft de ontwikkeling op het vlak van (versnelde) digitalisering. De strategie geeft hierbij ook aan dat dit heeft geleid tot een grotere urgentie van vragen rondom (digitale) veiligheid en privacy. De bron geeft ook aan dat gekwalificeerd ICT-personeel een belangrijke randvoorwaarde is voor de digitale transitie. De commissie constateert dat de voorgenomen opleiding studenten niet opleidt tot ICT'er, maar dat zij wel kennis zullen hebben van de digitale veiligheid waarover wordt gesproken in deze bron. De commissie is echter van mening dat de aanvrager onvoldoende duidelijk maakt hoe de aangehaalde informatie leidt tot een arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen opleiding en stelt dat deze bron daarom geen blijk geeft van een arbeidsmarktbehoefte aan dit type afgestudeerden.

Vervolgens verwijst de aanvrager naar de gegevens over de beroepen Security administrator, Cyber security specialist, ICT-consultant, Information Security Manager en Medewerker gegevensbeheer zoals deze zijn vermeld op de website van NationaleBeroepengids.nl (www.nationaleberoepengids.nl). Ook refereert de aanvrager aan de gegevens die zijn opgenomen in de Spanningsindicator van het UWV (www.werk.nl) betreffende beroepsgroepen bedrijfskundigen en organisatieadviseurs, beleidsadviseurs en managers ICT op zowel een landelijke als regionale schaal. De commissie merkt op dat de arbeidsmarkt begin 2020 is gekrompen als gevolg van de coronacrisis en dat deze krimp vervolgens is omgeslagen naar een (zeer) grote krapte op de arbeidsmarkt die zichtbaar is bij alle beroepsgroepen en alle sectoren. Het feit dat de arbeidsmarktspanning bij de door de commissie relevant geachte beroepsgroepen als (zeer) krap wordt getypeerd is daarom niet onderscheidend. De commissie kent daarom minder gewicht toe aan deze bronnen en stelt vast dat zij een (zeer) kleine positieve indicatie geven van een arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen opleiding.

De aanvrager beroept zich ook op verschillende rapporten van het UWV om de arbeidsmarktpositie van werknemers in verschillende beroepsgroepen te beschrijven. Het rapport 'Kansrijke beroepen' van het UWV (2021, p. 6, 8) geeft aan dat de beroepen

veiligheidsdeskundigen, security specialisten en netwerkbeheerders als kansrijk worden beschreven. Ook het rapport 'ICT-beroepen: Barometer arbeidsmarkt' van het UWV (2021, p. 2) beschrijft een aanhoudende krapte onder ICT-beroepen. De barometer herhaalt ook dat de beroepen security specialisten en netwerkbeheerders kansrijk worden geacht. Het factsheet 'Overheid: Factsheet arbeidsmarkt' van het UWV (2020, p. 4) vermeldt onder meer dat er een tekort is aan cybersecurityspecialisten bij de politie en defensie. In het rapport 'Moeilijk vervulbare vacatures en behoud van personeel: ervaringen werkgevers' van het UWV (2022, p. 2, 4) staat vermeld dat de sector informatie en communicatie in de top drie staat van sectoren met het hoogste aandeel moeilijk vervulbare vacatures. De aanvrager refereert ook aan het rapport 'Moeilijk vervulbare vacatures: Landelijk overzicht van beroepen' van het UWV (2019, p. 9) om aan te geven dat functies zoals security specialist, adviseur interne controle en beveiliging informatievoorziening ook al als moeilijk vervulbaar werden beschouwd. De commissie constateert dat deze bronnen in samenhang bezien blijk geven van een kwalitatieve arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen opleiding.

Ten slotte verwijst de aanvrager naar het arbeidsmarktonderzoek 'Marktpotentieel Master Digitale Veiligheid: Hogeschool Utrecht' dat in opdracht van de aanvrager is uitgevoerd door Lexnova (2022). Dit onderzoek is opgedeeld in een kwantitatief en een kwalitatief deel, die in verschillende deelrapportages zijn gepresenteerd door Lexnova.
De aanvrager refereert allereerst aan het kwalitatieve deel van het arbeidsmarktonderzoek, dat gebaseerd is op twaalf diepte-interviews die tussen april en juni 2022 zijn uitgevoerd. Het onderzoeksrapport bevat een overzicht van de functies van de respondenten en de bedrijven (of in enkele gevallen een omschrijving daarvan) waar zij voor werken. Transcripten van de interviews zijn tevens als bijlage meegeleverd. Hierbij wordt niet aangegeven welk transcript bij welke respondent hoort.
De geïnterviewden zijn positief over het opleidingsprofiel van de voorgenomen opleiding. Er wordt aangegeven dat het brede perspectief op het onderwerp digitale veiligheid waarbij veel aandacht bestaat voor generalistische (niet-technische) vaardigheden aanspreekt. Ook het opleidingsniveau wordt positief geëvalueerd. De geïnterviewden geven een positief beeld van de arbeidsmarktperspectieven voor afgestudeerden; meerdere respondenten geven aan dat er al een arbeidsmarktbehoefte bestaat en dat zij verwachten dat deze zal blijven groeien. Functies waarvan de respondenten denken dat afgestudeerden ervoor in aanmerking komen omvatten onder meer information risk manager, (chief) information security officer, risico manager en informatiebeveiliger.
De commissie acht het onderzoek valide en overwegend navolgbaar (de commissie kan bij één respondent niet bepalen of deze een uitspraak kan doen over het aannamebeleid van diens organisatie). De betrokken partijen maken het onderzoek ook voldoende relevant. De commisssie constateert dat het onderzoek een kwalitatieve arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen opleiding aantoont.

Ten slotte refereert de aanvrager aan het kwantitatieve deel van het arbeidsmarktonderzoek dat door Lexnova is uitgevoerd in de vorm van een online enquête die onder 104 werkgevers is afgenomen in juni en juli 2022. De respondenten zijn allemaal werkzaam voor organisaties die in Nederland zijn gevestigd; de meeste organisaties zijn gevestigd in Noord-Holland (26%), Gelderland (22%) en Noord-Brabant (19%). De respondenten zijn overwegend werkzaam in de sector informatie en communicatie (49%) en in de (specialistische) zakelijke dienstverlening (inclusief onderzoek) (24%). De organisaties verschillen sterk in grootte, maar de meeste respondenten werken voor bedrijven van 20-49 medewerkers (26%), 50-99 medewerkers (16%) of 100-199 medewerkers (15%). De respondenten zijn overwegend directeuren of eigenaren (67%) en werkzaam in senior management (15%) of middelmanagement (7%). 11% geeft aan een ander type functie te hebben. Een lijst van de hierbij genoemde functies is opgenomen in de bijlagen van het onderzoeksrapport.
Van de respondenten geeft 94% aan de voorgenomen opleiding (zeer) aansprekend te vinden en 77% is het (geheel) eens met de stelling dat er in hun werkveld een behoefte bestaat aan

afgestudeerden van de voorgenomen opleiding.
De respondenten is gevraagd of zij denken in de komende twee jaar een behoefte te hebben aan nieuwe medewerkers binnen de eigen organisatie die de voorgenomen opleiding hebben gevolgd. 42% van de respondenten verwacht een dergelijke behoefte, 26% van de respondenten verwacht deze niet en 32% weet niet of deze wordt verwacht. Deze respondenten zien een behoefte van minimaal 145 en maximaal 313 nieuwe medewerkers in de komende twee jaar. De commissie constateert dat bij de minimale behoefte één respondent minimaal 50 medewerkers aan te willen nemen. Ook heeft één (mogelijk dezelfde) respondent aangegeven maximaal 100 medewerkers aan te willen nemen in de komende twee jaar.
De respondenten is tevens gevraagd of zij denken een jaarlijkse behoefte te hebben aan de op- of bijscholing van huidige medewerkers. 45% van de respondenten geeft aan deze behoefte te hebben, 25% van de respondenten geeft aan deze behoefte niet te hebben en 30% weet niet of deze behoefte wordt verwacht. Deze respondenten zien een behoefte van minimaal 114 en maximaal 264 medewerkers die zij per jaar zouden willen opscholen. Ook hier constateert de commissie dat één respondent elk jaar minimaal 50 medewerkers zou willen opscholen en één (mogelijk dezelfde) respondent elk jaar maximaal 100 medewerkers zou willen opscholen door middel van de voorgenomen opleiding.
De commissie acht het arbeidsmarktonderzoek valide en overwegend navolgbaar. De navolgbaarheid wordt in de ogen van de commissie beperkt omdat de aanvrager een lijst van bedrijven heeft meegeleverd waarbij sommige ingevulde antwoorden niet duidelijk maken om welk bedrijf het gaat. Van sommige bedrijven is het ook niet duidelijk waarom zij een uitspraak kunnen doen over de behoefte aan afgestudeerden van de voorgenomen opleiding (zo is er een bedrijf dat aangeeft dat zij in de 'handel in hout en bouwmaterialen'-sector past en een dat zich in de 'tuinontwerpplatform'-sector schaart). Van tien van de respondenten is geen bedrijfsnaam vermeld. De commissie constateert verder dat niet alle respondenten met een 'andere' functie in een positie lijken te zijn om een uitspraak te doen over het aannamebeleid van hun organisatie. Omdat het dossier verder niet vermeldt welke respondent welke antwoorden heeft gegeven is het voor de commissie niet mogelijk te bepalen welke antwoorden relevant moeten worden geacht voor het bepalen van de arbeidsmarktbehoefte. Daarbij merkt de commissie op dat de vier hierboven bovengenoemde inschattingen van de kwantitatieve arbeidsmarktbehoefte (mogelijk van 1 respondent) significant afwijken van de overige inschattingen en dat de commissie niet in staat is om te verifiëren of deze afwijkende inschattingen reëel zijn. De commissie constateert dat het onderzoek een positieve indicatie geeft van de arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen opleiding.

De commissie concludeert op grond van het bovenstaande dat de aanvrager aannemelijk heeft gemaakt dat er een arbeidsmarktbehoefte bestaat aan de voorgenomen opleiding Digitale Veiligheid.

Beoordeling maatschappelijke behoefte
De aanvrager onderbouwt de maatschappelijke behoefte aan de hand van een groot aantal bronnen. De commissie neemt de volgende bronnen mee in de onderstaande overweging: de 'Strategische agenda hoger onderwijs en onderzoek: Houdbaar voor de toekomst' van het Ministerie van Onderwijs, Cultuur en Wetenschap (2019), het rapport 'Professionals voor morgen: Strategische agenda Vereniging Hogescholen 2019 - 2023' van de Vereniging Hogescholen (2019), de kamerbrief 'Informatie- en communicatietechnologie (ICT)' van de Staatssecretaris van Economische Zaken en Klimaat (2020, kamerstuk 26 643 nr 674), de kamerbrief 'Missiegedreven Topsectoren- en Innovatiebeleid' van de Staatssecretaris van Economische Zaken en Klimaat (26 april 2019), de 'Kennis- en innovatieagenda Veiligheid' van de Topsectoren (2019), de 'Kennis- en Innovatieagenda 2018-2021' van de Topsectoren (2017), de 'Nederlandse Cybersecurity Agenda' (2018) en de kamerbrief 'Voortgang Nederlandse Cybersecurity Agenda' (12 juni 2019).

Op grond van onder meer de 'Strategische agenda hoger onderwijs en onderzoek: Houdbaar voor

de toekomst' van het Ministerie van Onderwijs, Cultuur en Wetenschap (2019) en het rapport 'Professionals voor morgen: Strategische agenda Vereniging Hogescholen 2019 - 2023' van de Vereniging Hogescholen (2019) stelt de aanvrager dat er een algemene behoefte bestaat aan hbo masters. De commissie constateert dat deze bronnen blijk geven van een algemene behoefte aan hbo masters, waar de voorgenomen opleiding een voorbeeld van is.

De aanvrager gaat ook in op de maatschappelijke behoefte aan kennis van digitale veiligheid. Op grond van de kamerbrief 'Informatie- en communicatietechnologie (ICT)' van de Staatssecretaris van Economische Zaken en Klimaat (2020, kamerstuk 26 643 nr 674) stelt de aanvrager dat dit niet alleen van belang is binnen bètawetenschappen, maar ook binnen alfa- en gammawetenschappen. De kamerbrief 'Missiegedreven Topsectoren- en Innovatiebeleid' van de Staatssecretaris van Economische Zaken en Klimaat (26 april 2019) en de 'Kennis- en innovatieagenda Veiligheid' van de Topsectoren (2019, p. 56) gaan verder in op de relevantie van digitale veiligheid als het gaat om bescherming die nodig is om bijvoorbeeld het MKB te beschermen tegen cyberaanvallen. Deze bronnen wijzen op het belang van opleidingen op het gebied van digitale veiligheid om deze bescherming te waarborgen. De commissie constateert dat dit blijk geeft van een maatschappelijke behoefte aan de voorgenomen opleiding.

Verder wordt er verwezen naar de 'Kennis- en Innovatieagenda 2018-2021' van de Topsectoren (2017, p. 23-24), waarin wordt gesteld dat Nederland concurrerend moet blijven om zijn internationale toppositie te behouden en dat hierbij verschillende maatschappelijke vraagstukken opkomen. Eén van de hierin besproken maatschappelijke uitdagingen is 'de veilige samenleving', die heeft geleid tot de creatie van de hierboven genoemde Kennis- en Innovatieagenda Veiligheid (waarin ook de missie cyberveiligheid wordt besproken). Binnen de maatschappelijke uitdaging 'een veilige samenleving' wordt onder meer gesproken over het ontwerpen van veilige en betrouwbare informatiesystemen en de socio-economische factoren en ethiek van cybersecurity. De commissie stelt vast dat deze onderwerpen ook aan bod komen in de voorgenomen opleiding, wat blijk geeft van een maatschappelijke behoefte.

De 'Nederlandse Cybersecurity Agenda' (2018, p. 7, 16) wordt door de aanvrager aangehaald om te onderbouwen dat de overheid hierin het toenemende belang van cybersecurity in relatie tot de toenemende digitalisering benadrukt. In de agenda worden ambities genoemd op het gebied van digitale weerbaarheid. Hierin wordt onder andere de ambitie uitgesproken dat Nederland beschikt over weerbare digitale processen en een robuuste infrastructuur en dat Nederland beschikt over een integrale, publiek-private aanpak van cybersecurity. De agenda geeft ook aan dat kennis cruciaal is voor cybersecurity en dat er zowel fundamenteel als toegepast onderzoek naar dit onderwerp nodig is om de Nederlandse kennispositie te ontwikkelen. De kamerbrief 'Voortgang Nederlandse Cybersecurity Agenda' (12 juni 2019) bespreekt de voortgang van de agenda en geeft aan dat er nog meer concrete acties worden genomen om de digitale slagkracht te vergroten, zoals investeringen in personeel en expertise door middel van het werven van meer deskundigen. Ook geeft de kamerbrief aan dat er een intensivering nodig is op het gebied van onderwijs en kennisontwikkeling op het gebied van cybersecurity. De commissie constateert dat dit blijk geeft van een maatschappelijke behoefte aan de voorgenomen opleiding.

De commissie concludeert dat de aanvrager reeds op grond van het bovenstaande heeft aangetoond dat er een maatschappelijke behoefte bestaat aan de voorgenomen opleiding Digitale Veiligheid.

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
De commissie bepaalt het verwante opleidingenaanbod door vast te stellen welke bestaande opleidingen inhoudelijk sterk met de voorgenomen opleiding overeenkomen en opleiden 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. Ten slotte is voor de beoordeling van het verwant aanbod van belang om welke onderwijsvariant (voltijd, deeltijd of duaal) het gaat.

De aanvrager geeft allereerst aan dat er in de afgelopen jaren twee aanvragen zijn ingediend bij de CDHO voor hbo masters die de aanvrager "verwant" acht aan de voorgenomen opleiding. Het gaat hierbij om de hbo masters Cybersafety (NHL Stenden Hogeschool) en Cyber Security (Hogeschool van Amsterdam). De commissie constateert dat de macrodoelmatigheidsbesluiten voor deze nieuwe opleidingen zijn verlopen en dat, mochten deze instellingen deze opleidingen alsnog willen starten, zij een nieuwe macrodoelmatigheidstoets moeten doorlopen. De commissie weegt deze opleidingen daarom niet mee in de onderstaande overweging.

De aanvrager acht de hbo master Interdisciplinary Business Professional (Hanzehogeschool Groningen) "zijdelings verwant" aan de voorgenomen opleiding. Verder acht de aanvrager drie wo masteropleidingen "zijdelings verwant" vanwege daarin opgenomen tracks: de master Crisis and Security Management (Universiteit Leiden) vanwege de daarin opgenomen track Cyber Security Governance, de master Recht en Bestuur (Rijksuniversiteit Groningen) vanwege de daarin opgenomen track Governance and Law in Digital Society en de master Bestuurskunde (Rijksuniversiteit Groningen) vanwege de daarin opgenomen track Besturen van Veiligheid.
Ten slotte geeft de aanvrager aan dat er twee onbekostigde opleidingen zijn die "zijdelings verwant" zijn aan de voorgenomen opleiding: de hbo master Cyber Security Engineering (Haagse Hogeschool) en de wo master Cyber Security (Universiteit Leiden). De aanvrager geeft aan de instroom van deze opleidingen niet te weten en ze daarom niet te kunnen vermelden.
De aanvrager gebruikt in het dossier de termen “verwant” en "zijdelings verwant". Deze woorden worden door de commissie begrepen als vergelijkbaar met de door de commissie gebruikte termen "sterk verwant" en "aanverwant".

De commissie volgt de aanvrager in de afbakening van het verwante aanbod. De commissie volgt hierbij ook het argument van de aanvrager dat de technische wo-masteropleidingen die aandacht besteden aan cybersecurity onvoldoende verwant zijn omdat zij enkel toegankelijk zijn voor studenten met technische voorkennis, inhoudelijk slechts ten dele overlappen en studenten ook voor deels andere beroepen opleiden. De commissie kan de instroom in de verwante onbekostigde opleidingen niet meewegen omdat deze niet bekend zijn bij de commissie. De instroom van de tracks is voor de commissie ook niet bekend; om deze reden wordt in de onderstaande tabel de instroom in de (volledige) opleidingen waar de aanverwante tracks in worden aangeboden vermeld. De instroom in het aanverwante aanbod is in de afgelopen vijf jaar gestegen (zie Tabel 5).

Tabel 5. Instroom eerstejaarsstudenten in verwant bekostigd onderwijsaanbod

Opleiding	**Instelling**	**'17-'18**		**'18-'19**		**'19-'20**		**'20-'21**		**'21-'22**	
		VT	***DT***	***VT***	***DT***	***VT***	***DT***	***VT***	***DT***	***VT***	***DT***
M Interdisciplinary Business Professional (49291)	Hanzehogeschool Groningen (25BE), Groningen			27		26		37		24	15
M Bestuurskunde (66627)	Radboud Universiteit Nijmegen (21PM), Nijmegen	69		115		93		86		78	
M Crisis and Security Management (60417)	Universiteit Leiden (21PB), 's-Gravenhage	211		225		201		272		386	
M Recht en Bestuur (66461)	Rijksuniversiteit Groningen (21PC), Groningen	13	4	17	3	20	4	38	5	26	7
	Rijksuniversiteit Groningen (21PC), Leeuwarden			7		7		6		5	
Totaal Instroom		***293***	***4***	***391***	***3***	***347***	***4***	***439***	***5***	***519***	***22***

Bron: DUO

Vanaf 09/12/2022 is op de website van de CDHO kennisgegeven van het voornemen van de Hogeschool Utrecht om de hbo master Digitale Veiligheid in Utrecht aan te bieden. Hiermee is aan de instellingen voor hoger onderwijs de mogelijkheid gegeven om hun zienswijzen op dit voornemen kenbaar te maken. Op 19/12/2022 is er een zienswijze ingediend door Saxion Hogeschool.

Saxion Hogeschool geeft in haar zienswijze aan dat zij herkent dat digitale veiligheid een belangrijk maatschappelijk onderwerp is. Zij vermeldt hierop in te spelen door in samenwerking met de Universiteit Twente, de Politieacademie, het Nederlandse Instituut Publieke Veiligheid en de gemeente Apeldoorn een hbo masteropleiding op het gebied van digitale veiligheid vorm te geven, die zij beogen in Apeldoorn aan te bieden. Saxion Hogeschool geeft aan dat zij denkt dat goedkeuring van deze aanvraag haar kansen op een positief advies negatief kan beïnvloeden als de profielen van de opleidingen te veel overlappen. Saxion Hogeschool geeft aan contact te hebben gehad met de aanvrager om af te stemmen en mogelijk samen te werken. Saxion Hogeschool geeft aan dat het laatste overleg op 04/10/2022 heeft plaatsgevonden en dat hier is aangegeven dat de aanvrager beoogde deze aanvraag in het voorjaar van 2023 in te dienen. Saxion Hogeschool geeft aan dat haar aanvraag in een vergevorderd stadium is, maar dat zij op basis van de beschikbare samenvatting niet kan bepalen of de opleidingsprofielen overlappen en dat zij in contact wil treden met de aanvrager om de opleidingsprofielen op elkaar af te stemmen, mede omdat zij wil voorkomen dat er twee soortgelijke masters op een relatief beperkte geografische afstand van elkaar worden ontwikkeld. Saxion Hogeschool verzoekt de commissie hierbij om eerst ruimte te bieden tot afstemming voordat de commissie een oordeel velt over deze aanvraag.

De CDHO heeft de aanvrager op 20/12/2022 op de hoogte gesteld van de inhoud van de zienswijze en de gelegenheid gegeven om binnen tien werkdagen na ontvangst een reactie te geven. De aanvrager heeft op 22/12/2022 gereageerd. Hierin geeft de aanvrager allereerst aan het maatschappelijk belang van digitale veiligheid dat Saxion Hogeschool benoemt te herkennen. De aanvrager acht het van belang voor het werkveld om snel te handelen en de voorgenomen opleiding op zo'n kort mogelijke termijn aan te kunnen bieden.
De aanvrager erkent verder dat er gesprekken hebben plaatsgevonden met Saxion Hogeschool en NHL Stenden en dat hier inderdaad is gesproken over het afstemmen van de opleidingen. De aanvrager stelt te hebben aangegeven open te staan voor samenwerking, maar desondanks een eigen opleiding te willen starten. De aanvrager denkt verder dat, zelfs als Saxion Hogeschool op hetzelfde profiel inzet, er momenteel zo weinig bestaand aanbod is dat er voldoende arbeidsmarktbehoefte bestaat om beide opleidingen aan te bieden.
Ten slotte stelt de aanvrager dat samenwerking geen vereiste is volgens de Regeling. De aanvrager ziet geen grond in de Regeling voor Saxion Hogeschool om een zienswijze in te dienen omdat zij geen verwant aanbod aanbiedt en ook geen onderdeel uitmaakt van een erkend sectorplan. De aanvrager verzoekt de commissie daarom de aanvraag in behandeling te houden.

De commissie stelt voorop dat zij voorstander is van een goede samenwerking tussen de instellingen en betreurt dat het beschreven overleg niet heeft geleid tot een voor beide partijen bevredigende uitkomst.
De commissie stelt aanvragen niet buiten behandeling om nadere afstemming mogelijk te maken. De aanvrager heeft in haar reactie op de zienswijze aangegeven de aanvraag niet in te willen intrekken. De commissie kent verder geen gewicht toe aan de belangen van Saxion Hogeschool zolang zij geen aanvraag indienen of zijn aangesloten bij een erkend sectorplan.

De aanvrager heeft een prognose gemaakt van de instroom in de voorgenomen opleiding op grond van een enquête onder potentiële studenten die momenteel een hbo bacheloropleiding met betrekking tot veiligheid, ICT en recht bij de aanvrager volgen. De aanvrager verwacht dat er 20 studenten per jaar zullen instromen. De commissie acht deze prognose realistisch.

Als de instroom in de bestaande opleidingen en de verwachte instroom in de voorgenomen hbo master Digitale Veiligheid wordt afgezet tegen de maatschappelijke behoefte die bij criterium a is aangetoond en de arbeidsmarktbehoefte die daar aannemelijk is gemaakt, blijkt dat er voldoende ruimte is om deze opleiding binnen het bekostigde domein vorm te geven.

Vestiging van de opleiding in Utrecht heeft geen negatief effect op de landelijke spreiding van het onderwijsaanbod.

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

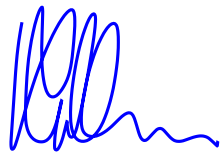
Gelet op het vorenstaande adviseert de Commissie Doelmatigheid Hoger Onderwijs u om positief te besluiten op het voorliggende verzoek. De commissie adviseert daarbij de toestemming te beperken tot de voltijdvariant op grond van de bevoegdheid in art. 6.2 lid 3 WHW.

Advies aan de NVAO over de naamkeuze en Croho indeling
De commissie heeft geconstateerd dat de voorgenomen opleiding dermate afwijkt van het bestaande verwante opleidingenaanbod, dat dit de keuze voor een andere naam rechtvaardigt.

Daarnaast heeft de commissie geconstateerd dat de aanvrager de hbo master Digitale Veiligheid in het Croho onderdeel Gedrag en maatschappij 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 opleidingenaanbod wordt voorzien.

Advies aan de NVAO over naamkeuze en Croho indeling
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 opleidingenaanbod voor studiekiezers 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 opleidingenaanbod voor studiekiezers 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.