De Haagse Hogeschool

M Cyber Security Engineering

Beperkte opleidingsbeoordeling

September 2023

Samenvatting

In juni 2023 is de bestaande tweejarige deeltijd masteropleiding Cyber Security Engineering (MSCE) van de Haagse Hogeschool bezocht door een visitatiepanel van NQA. De opleiding is **positief** beoordeeld: het panel concludeert dat aan alle standaarden wordt **voldaan**.

Schets van de opleiding
Het panel heeft kennis gemaakt met een deeltijd masteropleiding Cyber Security Engineering die onderscheidend is in Nederland door de focus op de technisch-organisatorische aspecten van cybersecurity in organisaties. De onbekostigde master is in februari 2019 van start gegaan en leidt professionals met minimaal twee jaar werkervaring op voor een adviserende rol als generiek technisch specialist in cybersecurity. De kleinschalige en daarmee studentgerichte opleiding heeft een instroom van 10 tot 15 studenten per jaar.

De beoogde leerresultaten
Het panel is positief over het heldere profiel van de MCSE met relevante interdisciplinaire componenten en een sterke verbinding met het werkveld. De opleiding baseert zich voor de leeruitkomsten op het beroepsprofiel ‘ICT-beveiligingsspecialist 3’ van het Platform voor Informatiebeveiliging (PvIB), dat bestaat uit vier vakgerichte en vier algemene competenties. De opleiding heeft dit overzichtelijk uitgewerkt in een competentiematrix met leeruitkomsten en bijbehorende criteria. De MCSE kent een kwalitatief hoogwaardige adviesraad die actief bijdraagt aan het actueel houden van het curriculum. De positie van de opleiding kan volgens het panel verder verstevigd worden door het versterken van het internationale perspectief en het aantrekken van niet-Nederlandstalige studenten met een Engelstalig onderwijsaanbod, mogelijk via een apart traject of met modulair onderwijs.

De onderwijsleeromgeving en de toetsing
De opleiding kent een duidelijk gestructureerd programma met drie thematische blokken en een goede balans tussen techniek en governance. Het team bestaat uit hoogopgeleide en kundige docenten, deels ook werkzaam in de praktijk, die veel individuele aandacht hebben voor de student en daarbij een waardevolle groepsdynamiek creëren. De opleiding kent goede feedback-processen en heeft een ontwikkelingsgerichte instelling. Er is veel aandacht voor onderzoek en studenten voelen zich hierdoor goed voorbereid op het afstudeertraject. Het panel ziet dan ook een optimale onderwijsleeromgeving waar veel uitwisseling tussen studenten en docenten plaatsvindt en men elkaar meeneemt in het leerproces. Verdere versteviging van het programma zal bereikt worden met hechtere samenwerking met de lectoraten, door meer expliciete aandacht voor ethiek in het gehele curriculum en sterkere regie op het laatste lesblok waarin veel gastcolleges plaatsvinden.

Er is een duidelijk toetsbeleid met beoordelingscriteria die zijn afgeleid van de competenties en leeruitkomsten en verantwoord worden in een toetsmatrijs. Er vinden zowel in- als externe kalibraties plaats, van waaruit verbeterpunten actief worden opgepakt. Het panel vindt de toetsing van het eindniveau goed geborgd waarbij het panel mogelijkheden ziet tot aanscherping van het beoordelingsformulier voor de technische beoordeling en vergroting van de rol van de praktijk in het beoordelingsproces.

De afstudeerfase
Het panel vindt het afstudeerproces helder van opzet. Studenten voeren in het laatste semester een opdracht uit waarin zij een complex vraagstuk op het gebied van cybersecurity analyseren en aanbevelingen formuleren. De eindwerken die het panel bestudeerd heeft, zijn van goede kwaliteit en representatief voor de opleiding. Het panel complimenteert de opleiding met de goede voorbereiding op het afstuderen, zij hoort en ziet dat onderzoek echt doorleefd is bij studenten. Het panel ziet kansen voor de opleiding om kennisdisseminatie te vergroten door verdergaande samenwerking op onderzoeksthema's met de lectoraten en door studenten te stimuleren publicaties of presentaties voor een breder (vak)publiek beschikbaar te stellen.

Tot slot
Het panel ziet een stevige, voor het werkveld relevante, masteropleiding met een ontwikkelingsgericht docententeam dat goed inspeelt op de snelle ontwikkelingen binnen het vakgebied. Zij ziet mooie kansen voor de opleiding om met de recente interne verhuizing naar de Faculteit IT & Design (in plaats van de positionering in de aparte The Hague Graduate School), de opleiding nog steviger te positioneren -mede door een hechtere samenwerking met de betrokken lectoraten- en daarmee de gewenste lichte groei te realiseren.

Inhoudsopgave

Inleiding

Dit visitatierapport bevat de beoordeling van de bestaande masteropleiding Cyber Security Engineering van de Haagse Hogeschool in Den Haag. Het visitatiepanel van NQA dat de beoordeling heeft uitgevoerd is samengesteld door NQA, in opdracht van de Haagse Hogeschool en in overleg met de opleiding. Voorafgaand aan de visitatie heeft de NVAO het panel goedgekeurd.

Het rapport beschrijft de bevindingen, overwegingen en conclusies van het panel. Ook bevat het een aanbeveling voor de opleiding. Het rapport is opgesteld conform het *Beoordelingskader accreditatiestelsel hoger onderwijs* van de NVAO (2018), de nadere uitwerking voor *Bijzondere kenmerken* (2017) van de NVAO en de *NQA Handleiding Opleidingsvisitaties Hoger Onderwijs 2022 Beperkte Opleidingsbeoordeling*.
De visitatie heeft plaatsgevonden op 27 juni 2023. Het visitatiepanel bestond uit:

De heer prof.dr.ir. B. (Bart) Preneel	Full professor KU Leuven, Dept. Electrical Eng.-ESAT, COSIC (voorzitter, domeindeskundige).
De heer dr.ir R.R. (René) Bakker	Lector Networked Applications, Academie IT en Mediadesign, HAN University of Applied Sciences (domeindeskundige).
De heer dr. D.J. van den Heuvel	Algemeen directeur/ondernemer Secura B.V. (werkvelddeskundige).
De heer ing. G.J.B. (Bryan) Laban	Student aan de hbo-masteropleiding Next Level Engineering aan Hogeschool Utrecht (student-lid).

Drs. P.R. (Patricia) Molegraaf, auditor van NQA, trad op als secretaris van het panel.

De opleiding Cyber Security Engineering is ingedeeld in de visitatiegroep HBO master Cyber Security Engineering. Afstemming tussen alle deelpanels heeft allereerst plaatsgevonden door de instructie die de panelleden krijgen met betrekking tot het beoordelingskader. De tussen Hobéon en NQA gekalibreerde criteria voor de beoordeling maken onderdeel uit van deze instructie. Daaraan voorafgaand is de afstemming geborgd door overlap in de bezetting tussen alle deelpanels. Daarnaast is, rekening houdend met het feit dat elke opleidingsbeoordeling een individuele beoordeling betreft, vanuit de overlap in de bezetting, waar relevant, voortschrijdend gereflecteerd op vorige bezoeken binnen deze visitatiegroep. De afstemming tussen de panels wordt verder geborgd door de ondersteuning van, zo veel mogelijk, dezelfde secretaris vanuit NQA en andere evaluatiebureaus en door de inzet van getrainde voorzitters.

Werkwijze panel en procesverloop
Voor de opleidingsbeoordeling heeft de opleiding een zelfevaluatie en bijlagen aangeboden. Voor de beoordeling van de gerealiseerde leerresultaten heeft het panel vijftien afstudeerdossiers van recent afgestudeerden bestudeerd. Deze dossiers zijn geselecteerd op basis van een groslijst van alumni van de afgelopen twee jaar (zie bijlage 2).

Centraal in de beoordeling stond het bezoek van het panel, bestaande uit deskundige *peers*. Twee weken voorafgaand aan het visitatiebezoek heeft het vooroverleg plaatsgevonden. In het overleg zijn de panelleden geïnstrueerd over de werkwijze van NQA en het NVAO-kader en zijn voorlopige bevindingen besproken. Zowel tijdens het vooroverleg als tijdens de visitatie zijn

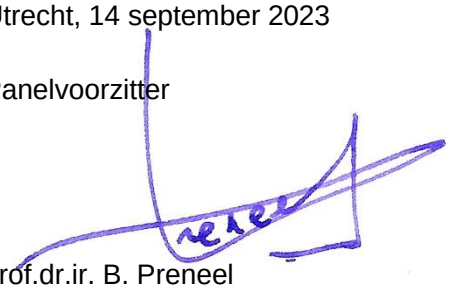
bevindingen voortdurend gedeeld. Tijdens het visitatiebezoek heeft het panel gesproken met diverse stakeholders van de opleiding, waaronder studenten, docenten (examinatoren) en vertegenwoordigers van het werkveld en is het ter inzage gelegde materiaal bestudeerd (zie bijlage 2). Aan het einde van de bezoekdag is de door het panel verkregen informatie verwerkt tot een totaalbeeld en tot een voorlopig oordeel met argumentatie. Tijdens een afsluitende mondelinge terugkoppeling heeft de voorzitter van het panel het eindoordeel en belangrijke bevindingen meegedeeld aan de opleiding. Medewerkers en studenten van de opleiding zijn in de gelegenheid gesteld om het panel (via mail) te benaderen buiten de bezoekdag om (inloopspreekuur). Er is van deze gelegenheid geen gebruik gemaakt.

Na het visitatiebezoek is een conceptrapportage opgesteld, dat is voorgelegd aan het panel. Met de input van de panelleden is een tweede concept opgesteld, dat ter controle op feitelijke onjuistheden is voorgelegd bij de opleiding. De panelleden hebben kennis genomen van de reactie van de opleiding en waar nodig zijn aanpassingen doorgevoerd. Vervolgens is het rapport definitief vastgesteld. Met alle (mondeling en schriftelijk) verstrekte informatie heeft het panel tot een weloverwogen oordeel kunnen komen.

Het visitatiepanel verklaart dat de beoordeling van de opleiding in onafhankelijkheid heeft plaatsgevonden.

Utrecht, 14 september 2023

Panelvoorzitter



prof.dr.ir. B. Preneel

Auditor

drs. P.R. Molegraaf

Schets van de opleiding / Karakteristiek

In februari 2019 is de onbekostigde deeltijd master Cyber Security Engineering (MCSE) van start gegaan. Inmiddels zijn vijf cohorten van deze studie gestart. De MCSE richt zich op de technisch-organisatorische aspecten van cybersecurity in organisaties. Het is daarmee de enige in Nederland; de Universiteit Leiden biedt een Executive Master Cyber Security aan maar deze focust op de bestuurlijk-organisatorische aspecten van cybersecurity in organisaties. De opleiding is ontwikkeld in samenwerking met de Universiteit Leiden, de Technische Universiteit Delft en diverse lectoraten binnen de Haagse Hogeschool. De MCSE leidt professionals met minimaal twee jaar werkervaring op voor een adviserende rol als technisch specialist in cybersecurity.

Tot september 2021 maakte de MCSE onderdeel uit van een aparte eenheid binnen de Haagse Hogeschool voor onderwijs aan professionals: de The Hague Graduate School (THGS). Deze is opgeheven om de opleidingen dichter bij het eigen kennisdomein en het aanverwante onderzoek en onderwijs te laten aansluiten. De MCSE is sindsdien opgegaan in de Faculteit IT & Design waar ook het kenniscentrum Cyber Security deel van uit maakt. De opleiding kent vanaf de start een redelijk stabiele instroom van 10 tot 15 studenten per jaar. De opleiding wil via alumni en met een grotere inspanning op marketing & communicatie inzetten op een iets groeiende instroom.

Opbouw opleiding
De MCSE heeft een omvang van 60 EC, verdeeld over twee studiejaren. Semester 1, 2 en 3 zijn ingedeeld in drie modules van 5 EC, semester 4 bestaat uit het afstudeeronderzoek. De lessen vinden plaats op vrijdag op de campus van The Hague Security Delta, een nationaal innovatiecentrum van het veiligheidscluster in Den Haag waar zowel bedrijven, overheden als kennisinstellingen gehuisvest zijn.

Basisgegevens opleiding

Naam opleiding in Centraal Register Opleidingen Hoger Onderwijs (CROHO)	Master Cyber Security Engineering
ISAT-code CROHO	70207
Oriëntatie en niveau opleiding	Hbo master
Graad	Master of Science (MSc)
Aantal studiepunten	60
Variant(en	Deeltijd 2 jaar (24 maanden)
Opleidingslocatie(s)	Den Haag
Onderwijstaal	Nederlands

Terugblik vorige visitatie
In 2018 is de Toets Nieuwe Opleiding (TNO) uitgevoerd. Als sterke punten noemde het panel het beroepsgerichte karakter en de breedte van de opleiding die met een stevig programma goed aansluit bij ontwikkelingen in de markt. In het rapport werd daarnaast een aantal aanbevelingen gegeven. Het panel ziet vanuit de ZER, de bestudeerde aanvullende documenten en de gevoerde gesprekken dat de opleiding deze serieus heeft opgepakt. Ook uit de actieve opvolging van adviezen vanuit de tussentijdse beoordeling van 2021 en de uitgevoerde risicoanalyse in 2022 blijkt een ontwikkelings- en kwaliteitsgerichte cultuur.

Uitgevoerde acties volgend op de aanbevelingen in de TNO en tussentijdse beoordeling zijn onder meer:

- Het aantal leerlijnen is teruggebracht naar één leerlijn, de leerlijn onderzoek. Daarnaast is het aantal leeruitkomsten bij de acht competenties verminderd waardoor het programma transparanter is geworden;
- Er is een ICT-lab opgezet op de HHs-vestiging in Delft waar uitgebreider en met speciaal voor dit lab geconfigureerde apparatuur geëxperimenteerd kan worden.
- Het aantal kerndocenten is uitgebreid van zes naar acht en door de verhuizing naar de Faculteit IT & Design is er een hechtere samenwerking op het gebied van onderzoek met de lectoraten. Twee lectoren zijn actief als docent binnen de master.
- Cybersecurity-deskundigheid is toegevoegd aan de examencommissie door lidmaatschap van een kerndocent van de MCSE.
- Alle leeruitkomsten zijn in de toetsmatrijzen gekoppeld aan de taxonomie van Bloom.

Beoordeling NVAO-standaarden

Standaard 1 Beoogde leerresultaten

De beoogde leerresultaten passen bij het niveau en de oriëntatie van de opleiding en zijn afgestemd op de verwachtingen van het beroepenveld en het vakgebied en op internationale eisen.

Conclusie

De opleiding **voldoet** aan de basiskwaliteit voor deze standaard.

Het panel concludeert dat de beoogde leerresultaten van de opleiding wat betreft niveau en oriëntatie voldoen aan het masterniveau NLQF7 en de eisen die het werkveld daaraan stelt. Voor de beoogde leerresultaten gaat de opleiding uit van PvIB-profiel 'ICT beveiligingsspecialist 3' met vier vakgerichte en vier algemene competenties. De opleiding heeft dit helder uitgewerkt in een competentiematrix met leeruitkomsten en bijbehorende criteria. Het panel is positief over het brede programma met goede interdisciplinaire componenten en de sterke verbinding met het werkveld. Kansen ziet het panel in het verstevigen van het internationale perspectief en het aantrekken van niet-Nederlandstalige studenten met een Engelstalig onderwijsaanbod, mogelijk via een apart traject of met modulair onderwijs, waarbij wel het sterke aspect van samen leren als groep in tact blijft.

Onderbouwing

Beroepsbeeld
De MCSE leidt studenten op voor het beroepsprofiel ‘ICT-beveiligingsspecialist 3’ van het Platform voor Informatiebeveiliging (PvIB), de beroepsvereniging van informatiebeveiligers en cybersecurity-professionals. Dit is het beroepsprofiel van een technische cybersecurityprofessional op masterniveau. De MCSE wil professionals opleiden tot technisch specialist in het domein van cybersecurity met de focus op een integrale benadering van cybersecurity waarbij de praktijkgeoriënteerde invalshoek gecombineerd wordt met een wetenschappelijke basis. Studenten hebben allen minimaal twee jaar werkervaring en zijn werkzaam in functies als ICT auditor, information security officer, senior adviseur informatiebeveiliging, cybersecurityspecialist en docent HBO-ICT. De ervaring van de opleiding is dat afgestudeerden zeer gewild zijn op de arbeidsmarkt. Ongeveer de helft van de studenten is tijdens of vlak na de studie van werkgever gewisseld en ook vindt vaak een carrièrestap binnen de eigen organisatie plaats.

Beoogde leerresultaten en profilering
De eindkwalificaties van de MCSE zijn gebaseerd op het bovengenoemde PvIB-profiel 'ICTbeveiligingsspecialist 3'. Dit profiel maakt gebruik van vier vakgerichte en vier algemene competenties, zie figuur 1. Het PvIB baseert zich op het European E-Competence Framework (E-CF) voor de uitwerking van vakspecifieke competenties op masterniveau. De acht competenties zijn uitgewerkt in leeruitkomsten op NLQF7 niveau met daarbij passende criteria. In een uitgewerkte competentiematrix is weergegeven hoe de competenties en leeruitkomsten gekoppeld zijn aan de modules en tevens hoe deze zich verhouden tot de Dublin descriptoren. Om het masterniveau te borgen is bij de ontwikkeling van de opleiding samengewerkt met de Universiteit Leiden, TU Delft en diverse partijen uit de praktijk zoals TNO, Cyberveilig Nederland, The Hague Security Delta, Nederlands Forensic Institute, en ABN AMRO.

Omdat cybersecurity een internationaal vakgebied is, is de opleiding ook internationaal georiënteerd qua literatuur, een deel van de praktijkcasussen en het gebruik van technische standaarden en documentatie op het gebied van security. De opleiding kiest daarbij wel voor Nederlands als voertaal binnen de opleiding omdat afnemende organisaties in de regio voornamelijk Nederlands als voertaal hebben.

	Competentie	Omschrijving
Vakgerichte competenties	1. Risicomanagement	De student is in staat om in een organisatie risicomanagement met betrekking tot de geautomatiseerde informatievoorziening te implementeren en uit te voeren.
	2. Informatiebeveiligingsmanagement	De student is in staat om voor een organisatie een informatie-beveiligingsbeleid op te stellen, de informatiebeveiligingsrisico's te beoordelen en de benodigde beveiligingsmaatregelen met betrekking tot de informatievoorziening en de ICT te implementeren, te monitoren, te toetsen, te evalueren en zo nodig aan te passen.
	3. Volgen van technologische ontwikkelingen	De student is in staat om op basis van grondige kennis met betrekking tot de IT de ontwikkelingen in de IT en cybersecurity te volgen en de kennis daarover uit te breiden.
	4. Oplossingen implementeren	De student is in staat om (cybersecurity)oplossingen in de ICT-infrastructuur, computers en software te implementeren, met inbegrip van installeren, beveiligen, actualiseren en buiten bedrijf stellen.
Algemene competenties	5. Onderzoek	De student is in staat om een wetenschappelijk onderzoek op te zetten, uit te voeren en de resultaten daaruit te publiceren.
	6. Analytisch vermogen	De student is in staat om complexe formuleringen samen te vatten, te conceptualiseren en te beoordelen, alsook redeneerfouten te herkennen en uit te leggen.
	7. Communicatie en overtuigingskracht	De student is in staat om bevindingen en standpunten te verwerken in een presentatie en adviesrapport voor specialisten en/of niet-specialisten met verschillende achtergronden en de bevindingen en standpunten mondeling en schriftelijk te verdedigen.
	8. Integriteit	De student kent de geschreven en ongeschreven normen, waarden en regels voor de werkomgeving en is in staat om daarnaar te handelen c.q. het goede voorbeeld te geven.

Figuur 1: Competentieprofiel Master Cyber Security Engineering.

Het panel concludeert dat de beoogde eindkwalificaties zoals geformuleerd door de opleiding in lijn zijn met wat mag worden verwacht van een professioneel masterniveau. Zij ziet een helder profiel met een goede interdisciplinaire component en een realistische lijst van competenties en leeruitkomsten. Het panel begrijpt dat de opleiding zich vooral richt op de PvIB beroepsprofielen omdat deze een meer technische insteek hebben dan de Europese ENISA profielen. Het panel adviseert de opleiding echter om met de op handen zijnde herziening van het PvIB beroepsprofiel het internationale perspectief te versterken door zich als opleiding duidelijker te verhouden tot de ENISA profielen en nog meer op een lijn te komen met nationale en internationale ontwikkelingen.[1] Hiermee wordt de stap naar openstelling voor een internationaal publiek eenvoudiger. Het panel wil de opleiding - vanwege het internationale karakter van het vakgebied - meegeven na te denken over het aanbieden van (delen van) de opleiding in het Engels, wellicht via modulair onderwijs.

[1] Zo zijn er twee belangrijke international richtlijnen: ACM/IEEE/AIS SIGSEC/IFIP Cybersecurity Curricular Guidelines, https://cybered.acm.org/ en The Cyber Security Body Of Knowledge https://www.cybok.org/

Afstemming met (internationale) beroepenveld

De opleiding zorgt op verschillende manieren voor een duurzame relatie met het werkveld: via het eigen docententeam, de leden van de Adviesraad MCSE en de eigen alumni. Vier van de acht kerndocenten en een groot deel van de docenten en gastdocenten zijn, naast hun werk als docent, werkzaam binnen de cybersecurity. Daarnaast zijn kerndocenten betrokken bij praktijkgericht onderzoek voor externe opdrachtgevers vanuit de kenniskring van de betrokken lectoraten. De Adviesraad komt twee tot drie keer per jaar bijeen en fungeert als sparringpartner van de opleiding en denkt mee over de actualiteit van het programma. Leden van de Adviesraad zijn onder andere werkzaam bij The Hague Security Delta, Cyberveilig Nederland, Randstad, Platform voor Informatiebeveiliging, Cybersecurity TNO en Digital Forensics NFI. Het panel is positief over de actieve rol en inbreng van de adviesraad. Zij ziet wel dat deze vrij sterk op Nederland gericht is en dat de balans industrie/overheid verbeterd zou kunnen worden. Ook via alumni wordt contact gehouden met het werkveld, enkelen zijn inmiddels (gast-)docent of afstudeerbegeleider in de opleiding. Input vanuit dit netwerk helpt het programma afgestemd te houden op behoeften en vragen vanuit het (internationale) beroepenveld.

Standaard 2 Onderwijsleeromgeving

Het programma, de onderwijsleeromgeving en de kwaliteit van het docententeam maken het voor de instromende studenten mogelijk de beoogde leerresultaten te realiseren.

Conclusie

De opleiding **voldoet** aan de basiskwaliteit voor deze standaard.

De opleiding kent een goed gestructureerd programma met een logische opbouw dat studenten in staat stelt zich succesvol te ontwikkelen tot een generiek technisch specialist. Het panel vindt de opzet van het programma goed aansluiten op de competenties en leeruitkomsten. Alumni en studenten zijn positief over de opleiding en de kundigheid en betrokkenheid van docenten. De opleiding heeft een positieve groepsdynamiek met veel aandacht voor de individuele student en diens leervragen. Onderzoek is goed belegd en ook over het ICT lab in Delft is het panel enthousiast. Het opleidingsteam is volgens het panel goed voorbereid op de voortdurende verandering van het vakgebied en heeft een ontwikkelingsgerichte instelling. Verbeterpunten worden dan ook snel opgepakt. Meer expliciete aandacht voor ethiek in het gehele curriculum en sterkere regie op het laatste lesblok waarin veel gastcolleges plaatsvinden, kunnen het programma verder verstevigen.

Onderbouwing

Onderwijsvisie en didactisch concept
De opleiding volgt de Haagse onderwijsvisie en kader voor professionals (2020) dat inzet op activerend, uitdagend en studeerbaar onderwijs. Het onderwijsconcept is een combinatie van theorie, praktijkvoorbeelden en onderzoek, toegepast binnen de werkomgeving van de student. Omdat cybersecurity een zich snel ontwikkelend vakgebied is, worden in elke module casestudies uit de praktijk ingebracht, afkomstig van de studenten en/of uit het netwerk van de docenten. Daarnaast wordt het onderwijs ingevuld in samenwerking met lectoren, het kenniscentrum cybersecurity en het werkveld middels een groot aandeel van gastcolleges. Er is bewust gekozen voor fysieke lessen op locatie, waarbij online materiaal beschikbaar is via de digitale leeromgeving. Een onderdeel hiervan is een lab-omgeving waarin de studenten pentests kunnen uitvoeren, ICT-beveiligingsconfiguraties onderzoeken en cyberaanvallen analyseren. Studenten en alumni waar het panel mee gesproken heeft, zijn zeer positief over de meerwaarde van de samenwerking en uitwisseling met medestudenten op locatie tijdens de lessen en het uitwerken van opdrachten. Als voorbeeld noemen zij dat studenten werkzaam bij Stedin hun praktijkervaring inbrengen bij een les over Operational Technology. Het kleinschalige onderwijs maakt dat docenten goed kunnen afstemmen op de ervaring en achtergrond van studenten. Naast (gast)colleges en (lab)workshops vinden tijdens elke module verschillende werksessies plaats. Deze opzet, waarin studenten zich in korte tijd moeten verdiepen in een thema en dit vervolgens presenteren aan de groep, leert studenten zich snel nieuwe ontwikkelingen eigen te maken: bij uitstek relevant binnen dit vakgebied. Het panel ziet een optimale onderwijsleeromgeving waar veel uitwisseling tussen studenten en docenten plaatsvindt en men elkaar meeneemt in het leerproces.

Opzet en inhoud programma
De MCSE bestaat uit vier semesters van elk 15 EC. De eerste drie semesters bestaan uit drie modules van 5 EC (zie figuur 2). Elke module is opgebouwd uit een aantal vakken en één of

meer projectopdrachten en sluit af met een schriftelijke toets en/of een projectassessment. In het vierde en laatste semester voert de student zelfstandig een praktijkgericht onderzoek uit en schrijft een thesis. De studielast bestaat uit één dag onderwijs op de The Hague Security Delta en 12 uur zelfstudie.

Figuur 2. Schematisch overzicht curriculum MCSE.

De negen modules zijn opgebouwd als ‘sandwich’: de eerste drie modules geven algemene kennis over cybersecurity en governance en leggen de basis, de middelste drie zijn technisch van aard en de laatste drie leggen de koppeling naar de beroepspraktijk. De opleiding leidt op tot generieke technisch specialist. De eerste drie modules worden ook benut om alle studenten op een zelfde niveau te brengen vanuit de verschillende achtergronden van waaruit zij instromen. De daaropvolgende drie modules bevatten een laboratoriumomgeving voor specifieke cybersecurityonderdelen zoals software, malware, hacking en monitoring. Module 7, 8 en 9 zijn gericht op (onderzoek in) de beroepspraktijk in verschillende sectoren zoals financiële dienstverlening, zorg en vitale voorzieningen.

Het panel ziet dat de opbouw van het programma met de drie blokken een goede balans kent tussen techniek en governance. Sommige studenten zouden iets meer aandacht voor techniek in het programma willen zien maar het panel vindt het goed dat de opleiding, vanuit techniek, breed kijkt naar de betekenis voor de bedrijfsvoering. Zij ziet een in de kern technische opleiding die wel continu multidisciplinaire elementen integreert. Aandachtspunt is de inrichting van het derde blok met de modules 7, 8 en 9. Deze modules kennen veel externe sprekers waar onderlinge afstemming verbeterd kan worden om overlap en herhaling te voorkomen. De opleiding is zich hier van bewust en werkt al aan verbetering. Een strakkere regie en meer inzet van vaste kerndocenten zal zorgen voor betere samenhang en afstemming. Het panel vindt de brede inzet van gastdocenten hierbij wel een belangrijke meerwaarde.
Daarnaast adviseert het panel de opleiding ethiek explicieter aandacht te geven in het curriculum. Het komt aan bod in twee modules, met onderwerpen als AVG en monitoring, en daarnaast is er impliciet aandacht voor ethische vraagstukken. Het panel zou meer specifieke aandacht willen zien voor ethische vraagstukken zoals wat is ethisch verantwoord, wanneer is sprake van cybercriminaliteit, wat betekent veilig. Het panel vindt het belangrijk dat studenten bewust leren

kijken vanuit een ethisch standpunt, waarbij ethiek ook explicieter onderdeel is van het afstuderen.

Onderzoeksvaardigheden
Het panel ziet dat onderzoek en onderzoeksvaardigheden goed belegd zijn binnen de opleiding. De opleiding benadrukt het belang van bruikbaarheid van de verkregen onderzoeksresultaten. Er wordt daarom in het onderwijs nadruk gelegd op het vertalen van de onderzoeksresultaten naar ideeën, oplossingen, adviezen en producten die binnen de beroepspraktijk kunnen worden gebruikt. Er loopt een onderzoeksleerlijn door het gehele curriculum waardoor in elke module onderzoeksmethodiek belegd is en altijd één lesdag besteed wordt aan een bepaalde onderzoekstechniek. Studenten voelen zich goed voorbereid op het afstudeertraject, nog meer doordat het formuleren van het onderzoeksvoorstel sinds dit studiejaar naar voren is gehaald naar module 8 in plaats van module 9. De voorgenomen verdere verbinding met de lectoraten gekoppeld aan het Kenniscentrum Cyber Security moedigt het panel aan. Afstudeerthema's zouden meer verdiept kunnen worden als zij gekoppeld worden aan onderzoeksthema's van de lectoraten.

Studeerbaarheid en studieloopbaanbegeleiding
Elke student start met een uitgebreid intakegesprek waardoor de opleiding een goed beeld krijgt van de voorkennis van de student en kan beoordelen of de studie passend is. Na de start voert de teamleider individuele gesprekken over studievoortgang en eventuele belemmeringen. Omdat de studentenomvang klein is, zijn docenten nauw betrokken en is er veel persoonlijke begeleiding. Studenten en alumni waarmee het panel sprak, ervaren dit ook zo. Daarnaast is de samenwerking onderling tussen studenten hecht en versterkt dit de binding met de opleiding.
Er is niet veel uitval, mede vanwege de bewuste keuze voor deze onbekostigde studie en de instroomeis van twee jaar werkervaring. De grootste oorzaak van uitval die plaatsvindt, is het ontbreken van technische kennis. Het panel vindt het goed dat de opleiding hier aandacht voor heeft en dit wil ondervangen door het verscherpen van de intake- en voorbereidingsprocedure.

Docenten
Het docententeam bestaat uit een vaste groep van acht kerndocenten, een teamleider en een opleidingsmanager. Zes docenten zijn gepromoveerd en allen, met uitzondering van de lector Cyber Security die een eerstegraads onderwijsbevoegdheid heeft, hebben de Basis Kwalificatie Examinering (BKE) behaald. De acht kerndocenten zijn elk eindverantwoordelijk voor een van de negen modules. Daarnaast wordt gewerkt met verschillende docenten die een aantal collegedagen verzorgen. De opleiding heeft twee jaar geleden de 'docentenpool' uitgebreid met drie nieuwe docenten, allen alumni, die af en toe colleges geven en invallen als een kerndocent uitvalt. Daarnaast zijn zij afstudeerbegeleider. Zo wil de opleiding een bredere groep potentiële docenten creëren en daardoor minder kwetsbaar zijn bij ziekte of uitval. Het panel vindt dit goede initiatieven die tegelijk zorgen voor binding met alumni en actualisering van het curriculum vanuit docenten in de praktijk. Het panel ziet daarbij een kundige en gevarieerde groep kerndocenten met goede technische diepgang, waar studenten zeer enthousiast over zijn.

Standaard 3 Toetsing

De opleiding beschikt over een adequaat systeem van toetsing.

Conclusie

De opleiding **voldoet** aan de basiskwaliteit voor deze standaard.

Het panel vindt het toetsprogramma van de opleiding logisch opgebouwd met een goede verhouding tussen tentamens en praktijkopdrachten, en groeps- en individueel werk. Er is een duidelijk toetsbeleid met beoordelingscriteria die zijn afgeleid van de competenties en leeruitkomsten, verantwoord in een toetsmatrijs. Studenten geven aan dat zij goed voorbereid worden op hun toetsen. Het panel vindt de toetsing van het eindniveau goed geborgd waarbij het panel nog kansen ziet tot aanscherping van het beoordelingsformulier voor de technische beoordeling en vergroting van de rol van de praktijk in het beoordelingsproces. De kwaliteit van de toetsing wordt goed geborgd met een gemandateerde Kamer voor Masteropleidingen en toetscommissies die steekproefsgewijs onderzoek uitvoeren. Het panel is positief over de vele kalibraties, zowel binnen als buiten de opleiding, en de actieve opvolging van de verbeterpunten die hieruit voortkomen.

Onderbouwing

Toetsbeleid
De opleiding volgt het toetsbeleid en richtlijnen voor het toetsproces van de Haagse Hogeschool. Toetsen worden ingezet om het leren te stimuleren en om beslissingen over studievoortgang te onderbouwen. Er wordt zowel summatief als formatief getoetst waarbij de student feedback en feedforward krijgt voor het vervolgtraject. Bij groepsproducten wordt in een mondeling assessment vastgesteld of iedere student de te behalen competenties voldoende heeft aangetoond. De beoordelingscriteria zijn afgeleid van de competenties en leeruitkomsten en verantwoord in een toetsmatrijs. Het panel constateert dat de opleiding een helder toetsbeleid heeft met duidelijke doelstellingen en principes.

Toetsuitvoering
De toetsing bestaat in het eerste jaar, voor module 1 tot en met 6, uit een schriftelijke toets -vaak een tentamen- gecombineerd met groeps- en/of individuele (lab)opdrachten en een eindpresentatie. De tentamens toetsen kennis en het kunnen toepassen van de verkregen kennis. In het tweede jaar, in module 7,8 en 9, werken studenten praktijkopdrachten uit, in duo's of alleen, die worden gepresenteerd aan elkaar en de examinatoren. Gedurende de modules zijn er meerdere feedbackmomenten ingeroosterd waarin studenten begeleid worden bij het maken van de schrijfopdrachten. Studenten zijn tevreden over de wijze van toetsing en voelen zich goed begeleid, meeloopgedrag komt niet voor omdat studenten elkaar aanspreken en stimuleren.
Het panel heeft van alle negen modules toetsen ingezien en ziet een goede opbouw in toetsing met een mooie verhouding tussen tentamens en praktijkopdrachten, en groeps- en individueel werk. De toetsen die het panel heeft ingezien zijn van een goed niveau en worden adequaat beoordeeld. Studenten geven aan tentamens een belangrijk onderdeel te vinden van de toetsing die hen stimuleren verdieping te 'pakken'.

Toetsing afstuderen
Studenten kunnen starten met het afstuderen als zij 45 EC hebben behaald en een met voldoende beoordeeld onderzoeksvoorstel hebben opgesteld. De toetsing bestaat uit de masterthesis en mondelinge verdediging, beoordeeld in een beoordelingsformulier met een eindbeoordeling op een schaal van 1 tot 10. De mondelinge verdediging telt voor 10% van het eindcijfer mee en vindt plaats als de masterthesis is ingeleverd en als voldoende beoordeeld.

Om het eindniveau te borgen vindt in- en externe borging plaats. Interne borging vindt plaats door periodieke kalibraties tussen examinatoren, het werken in verschillende samenstellingen van examinatoren en kalibratiesessies door leden van de examencommissie waarvan de laatste in het voorjaar van 2023 heeft plaatsgevonden. Periodiek wordt eveneens door externe borging gekeken of het eindniveau gerealiseerd wordt, bijvoorbeeld door het voorleggen van theses aan externe deskundigen. In het voorjaar van 2023 zijn kalibratiesessies georganiseerd met de Universiteit van Amsterdam en de Hogeschool Leiden waarin werken van de laatste twee cohorten voorgelegd zijn. Naar aanleiding van de interne en externe kalibraties van het voorjaar heeft de opleiding diverse onderdelen in het beoordelingsformulier aangepast. Er is bijvoorbeeld een duidelijkere rubric opgesteld met cijfer-ranges ter ondersteuning van de transparantie van de beoordeling en voor alle 10 criteria is de norm gesteld op minstens 5 waarbij het eindcijfer minstens 5,5 moet zijn. Daarnaast is het toetsonderdeel zelfevaluatie duidelijker gekoppeld aan de leeruitkomsten. Het panel is positief over de in- en externe kalibraties en de actieve wijze waarop de opleiding verbeterpunten oppakt. Uit de externe kalibratie werd duidelijk dat er verschil in beoordeling ontstond doordat de technische beoordeling nu niet expliciet in het meer generieke beoordelingsformulier is opgenomen. Het panel beveelt de opleiding daarom aan deze hierin wel te expliciteren. Naast de onderzoekskwaliteiten is het technische niveau van de student ten slotte ook een belangrijk aspect dat nu vooral impliciet bij de examinatoren ligt.

Het panel vindt het passend dat de opleiding zich richt op praktijkgericht onderzoek, waarbij de uitkomsten van het onderzoek een bijdrage dienen te leveren aan de beroepspraktijk van de student en anderen. Met de examencommissie ziet het panel dat deze praktische bruikbaarheid alleen wordt beoordeeld door de examinatoren van de opleiding; er wordt geen advies vanuit het werkveld betrokken bij dit oordeel. Het panel adviseert de opleiding dan ook om de bedrijfsbegeleider actiever in het beoordelingsproces te betrekken, bijvoorbeeld door deze advies te vragen middels een vragenlijst vooraf.

Borging kwaliteit toetsing
Het panel concludeert dat de toetskwaliteit goed wordt geborgd door het volgen van de richtlijnen voor het toetsproces. In de toetsmatrijs wordt de koppeling tussen leerdoelen, niveau en toetsvormen vastgelegd. Toetsen worden ontwikkeld door de kerndocenten waarbij het vierogen-principe wordt toegepast en alle toetsen door een tweede teamlid beoordeeld worden. Na iedere toetsafname vindt een evaluatie plaats. Bespreekpunten over toetsen worden door de kerndocenten in de curriculumcommissie besproken. Voor elke schriftelijke toets zijn de toetsmatrijs, de toetsvragen en een antwoordmodel beschikbaar. Alle kerndocenten beschikken over de Basiskwalificatie in Examinering (BKE) of zijn vrijgesteld daarvan (zie standaard 2). Examinatoren worden benoemd door de examencommissie. Bij assessments worden twee examinatoren ingezet. De masterthesis wordt eveneens door twee examinatoren beoordeeld. Elk semester wordt daarbij gekalibreerd met betrokken examinatoren. Bij de uitvoering en controle van toetsing zijn behalve de toetscommissie en de examencommissie ook de curriculum- en opleidingscommissie betrokken. De curriculumcommissie benoemt en evalueert de

leeruitkomsten en bijbehorende toetsing en stelt deze bij indien nodig. De opleidingscommissie geeft advies over de studeerbaarheid van het programma waaronder toetsing.

Sinds studiejaar 2022-2023 valt de opleiding onder de examencommissie van de Faculteit ITD. De opleiding is via een Kamer voor Masteropleidingen in de examencommissie van ITD vertegenwoordigd. Een docent van de MCSE met specialistische expertise op het gebied van cybersecurity engineering is lid hiervan. De voorzitter van de examencommissie is tevens voorzitter van de kamer. De examencommissie is onder meer verantwoordelijk voor borging van de kwaliteit van toetsen en examens en heeft een deel van deze activiteiten gedelegeerd aan de toetscommissie. De MCSE heeft een eigen toetscommissie, die onder toezicht en verantwoordelijkheid van de examencommissie belast is met de controle op de naleving van het toetsbeleid. Het panel concludeert op basis van bestudeerde documenten en de gevoerde gesprekken dat examencommissie en toetscommissie naar behoren functioneren en zorgen voor voldoende borging van het eindniveau.

Standaard 4 Gerealiseerde leerresultaten

De opleiding toont aan dat de beoogde leerresultaten zijn gerealiseerd.

Conclusie

De opleiding **voldoet** aan de basiskwaliteit voor deze standaard.

Het afstudeerprogramma stelt studenten in staat om de beoogde leerresultaten te behalen. Studenten tonen met een masterthesis en eindpresentatie aan het gewenste NLQF7-niveau te beheersen. De bestudeerde eindwerken van de opleiding zijn van goed niveau en behandelen relevante thema's uit het vakgebied. De opzet en theoretische en methodologische onderbouwing van de theses zijn goed waarbij in sommige werken interdisciplinaire en ethische aspecten meer aan bod mogen komen. Kennisdisseminatie zal versterkt worden door de voorgenomen sterkere samenwerking met de lectoraten waardoor onderzoeksthema's verder uitgewerkt en verdiept kunnen worden. De opleiding mag van het panel meer sturen op publicaties in vakbladen en externe presentaties. Deze kwalitatief hoogwaardige en relevante master zou daarmee tevens aan bekendheid kunnen winnen.

Onderbouwing

Het afstudeerproces
Het panel vindt het afstudeerproces helder van opzet. Uit de gevoerde gesprekken blijkt dat studenten zich goed voorbereid en begeleid voelen. In de onderzoekslijn, die door het gehele curriculum loopt, hebben studenten alle stappen van het opzetten en uitvoeren van onderzoek doorlopen en tevens geoefend met het schrijven van papers. Alle competenties zijn reeds getoetst bij aanvang van het afstuderen maar met de masterthesis toont de student aan zelfstandig een geheel onderzoektraject te kunnen doorlopen. Studenten voeren in het laatste semester een opdracht uit waarin zij een complex vraagstuk op het gebied van cybersecurity analyseren en aanbevelingen formuleren. De voorbereiding van het afstuderen zit in module 8 waar studenten een onderzoeksvoorstel ter goedkeuring voorleggen aan de onderzoekscoördinator. Het panel complimenteert de opleiding met de goede voorbereiding op het afstuderen, zij hoort en ziet dat onderzoek echt doorleefd is bij studenten.

Producten van afgestudeerden
Het panel heeft vijftien afstudeerrapporten met bijbehorende beoordelingen bestudeerd. Zij vindt de bestudeerde eindwerken van goede kwaliteit en representatief voor het vakgebied. De opzet en theoretische en methodologische onderbouwing van de theses zijn goed. In een deel van de onderzoeken zou volgens het panel wel meer aandacht besteed kunnen worden aan interdisciplinaire en ethische aspecten. Het panel begrijpt dat de afstudeerwerken, doordat deze gekoppeld zijn aan de werkplek van de student, een wat geïsoleerde positie hebben, ook vanwege de eerdere positionering in de The Hague Graduate School. Met de verhuizing naar de Faculteit ITD en de dichtere positie bij de lectoraten ziet het panel kansen voor grotere kennisdisseminatie door een sterkere koppeling van onderzoeksthema's aan die van de lectoraten. Daarbij vindt het panel de theses omvangrijk en zou zij het een goede aanvulling vinden als studenten de mogelijkheid krijgen een korter afstudeerrapport in te leveren als zij daarbij een publicabel artikel voor een vakblad of wetenschappelijk tijdschrift aanleveren. Het panel zou het mooi vinden als deze relevante en kwalitatief hoogwaardige masteropleiding door

de publicatie van de afstudeerrapporten (of ten minste samenvattingen ervan), artikelen over de theses en middels presentaties van afstudeeronderzoeken op kennisbijeenkomsten, meer bekendheid zou krijgen. Om zo te tonen aan de beroepspraktijk dat er origineel (soms grensverleggend) werk wordt opgeleverd met een praktisch-wetenschappelijke inslag. Relevante en actuele onderzoeksonderwerpen die het panel heeft gezien zijn bijvoorbeeld ‘Assessing vulnerability Risk For Industrial Control Systems’ en identificatie van applicaties in HTTP/3-verkeer. Ook het onderzoek naar de baseline Informatiebeveiliging Overheid (BIO) en de Azure Stack Hub omgeving binnen de Rijksoverheid gaat duidelijk over een student die zijn/haar kennis heeft toegepast in een concrete setting (Microsoft Azure) in diens werkomgeving.

Functioneren afgestudeerden
Alumni zijn tevreden over de opleiding. Zij vinden het van meerwaarde dat ze vanuit de studie en het uitgevoerde onderzoek nieuwe kennis inbrengen in hun werk en organisatie. Daarnaast leren ze veel van het meekijken ‘over de schutting’ bij medestudenten en hun werkplek. De leden van de adviesraad geven aan dat de opleiding voorziet in een grote behoefte aan mensen in het brede werkveld. Het onderscheidende is volgens hen dat deze opleiding gericht is op cyber security *engineering*, met hands on elementen, gericht op ook echt ‘doen en maken’. Alumni blijven met elkaar in contact en vormen een hechte community met elkaar. Zij worden bij het onderwijs betrokken via gastcolleges of docentschap. Een klein deel van de studenten start na de studie een PhD traject. Dit traject moet nu gestart worden via een universiteit waar de positie van professionele masters nog niet overal voldoende (h)erkend wordt. De komst van professional doctorates met een andere invulling van de derde cyclus, kan een aantrekkelijk alternatief zijn voor afgestudeerde MSCE studenten.

Eindoordeel over de opleiding

	Master Cyber Security Engineering
Standaard 1 Beoogde leerresultaten	Voldoet
Standaard 2 Onderwijsleeromgeving	Voldoet
Standaard 3 Toetsing	Voldoet
Standaard 4 Gerealiseerde leerresultaten	Voldoet

De oordelen zijn gewogen volgens de beslisregels van de NVAO. Op basis hiervan beoordeelt het visitatiepanel de kwaliteit van de deeltijd Masteropleiding Cyber Security Engineering in Den Haag als **positief.**

Aanbevelingen

Standaard 3

- Neem de criteria voor de technische beoordeling expliciet op in het beoordelingsformulier afstuderen.

Het panel wil de opleiding daarbij de volgende **adviezen/aanmoedigingen**[2] meegeven:

- Het panel adviseert de opleiding om met de op handen zijnde herziening van het PvIB beroepsprofiel het internationale perspectief te versterken door zich als opleiding duidelijker te verhouden tot de ENISA profielen en nog meer op een lijn te komen met nationale en internationale ontwikkelingen.

- Het panel wil de opleiding meegeven na te denken over het aanbieden van - delen van - de opleiding in het Engels, wellicht via modulair onderwijs.

- Het panel adviseert de opleiding ethiek explicieter aandacht te geven in het curriculum.

- De voorgenomen verdere verbinding met de lectoraten van het Kenniscentrum Cyber Security moedigt het panel aan. Afstudeerthema's zouden meer verdiept kunnen worden als zij gekoppeld worden aan onderzoeksthema's van de lectoraten.

- Het panel adviseert de opleiding om de bedrijfsbegeleider actiever in het beoordelingsproces te betrekken.

[2] **Aanbevelingen** zijn zwaarwegender in kader van de verbeterfunctie en versterking van de basiskwaliteit. Daar moet een opleiding zich bij een volgende visitatie op verantwoorden.
Adviezen zijn lichter van gewicht en gericht op ontwikkelmogelijkheden bovenop de basiskwaliteit.
Aanmoedigingen zijn een bevestiging van een ontwikkeling/koers die een opleiding al heeft ingezet.

Deel III

Bijlagen

1. Bezoekprogramma

Tijdstip		Aanwezigen
09.45 uur – 10.00 uur	Ontvangst panel door management opleiding	– Directeur Faculteit IT&D – Opleidingsmanager IT&D Pro en ADS&AI – Programmamanager MSCE
10.00 uur – 11.00 uur	Gesprek docenten	– Lector en kerndocent – Kerndocent – Kerndocent - Onderwijskundige dienst OKC
11.00 uur – 11.15 uur	Pauze	
11.15 uur – 12.00 uur	Gesprek studenten	– Student cohort 2022-2024 – Student cohort 2022-2024 (OC lid) – Student cohort 2022-2024
12.00 uur – 13.00 uur	Lunch	
13.00 uur – 13.45 uur	Gesprek Adviesraad, alumni en Opleidingscommissie	– Voorzitter Adviesraad MSCE – Lid Adviesraad MSCE – Lid Adviesraad MSCE – Opleidingscommissie IT&D Pro – Alumnus cohort 2020-2022 – Alumnus cohort 2020-2022
13.45 uur – 14.00 uur	Pauze	
14.00 uur – 14.45 uur	Gesprek opleidingsmanagement	– Directeur Faculteit IT&D – Opleidingsmanager IT&D Pro + ADS&AI – Programmamanager MSCE
14.45 uur – 15.00 uur	Pauze	
15.00 uur – 15.45 uur	Gesprek Examencommissie en Toetscommissie	– Voorzitter Examencommissie IT&D – Voorzitter Examencommissie THGS – Kerndocent / lid Examencommissie, voorzitter Toetscommissie
15.45 uur – 16.45 uur	Beoordelingsoverleg panel	
16.45 uur – 17.00 uur	Terugkoppeling	

2. Bestudeerde documenten

Zelfevaluatie Master Cyber Security Engineering
Opleidingskader MCSE 2023
MSCE OER & OLP 2023-2024
Onderwijsvisie & Kaders Professionals
MCSE Competentiematrix 2023
De Haagse Toetsing 2019
Toetshandboek Masteropleidingen THGS
PvIB Beroepsprofiel ICT Beveiligingsspecialist
Leerlijn onderzoek in de MCSE
De HHs Onderzoekend leren met impact. Instellingsplan 2023-2028
Overzicht en cv's betrokken personeel
Jaarverslag ITD Examencommissie 2021-2022
Jaarverslag THGS Masters Examencommissie 2021-2022
Kalibratie Theses MCSE 2023
Totaal overzicht BKE status docenten MCSE
Notulen Adviesraad
Notulen Opleidingscommissie
PDCA Matrix MCSE 2022 en 2023
MCSE Studiehandleidingen module 1 t/m 9
MCSE Afstudeerhandleiding, module 10
Selectie van toetsen vanuit elke module (1 t/m 9)
Afstudeerdossiers inclusief studentproducten en beoordelingen van acht studenten afstudeercohort 2020-2022
Afstudeerdossiers inclusief studentproducten en beoordelingen van zeven studenten afstudeercohort 2021-2023