Uddannelses- og Forskningsministeriet

Prækvalifikation af videregående uddannelser - Cybersikkerhed og risikohåndtering

Udskrevet 5. september 2026

Master - Cybersikkerhed og risikohåndtering - Syddansk Universitet

Institutionsnavn: Syddansk Universitet
Indsendt: 15/09-2025 07:47
Ansøgningsrunde: 2025-2
Status på ansøgning: Godkendt
Afgørelsesbilag
Download den samlede ansøgning
Læs hele ansøgningen

Ansøgningstype
Ny uddannelse

Udbudssted
SDU Odense

Informationer på kontaktperson for ansøgningen (navn, email og telefonnummer)
AC-generalist Sabine Gantzhorn Hildebrand, 65 50 21 36, sabh@sdu.dk, Det Naturvidenskabelige Fakultetssekretariat, SDU. Samt SDUs prækvalifikations mailbox praekval@sdu.dk.

Er institutionen institutionsakkrediteret?
Ja

Er der tidligere søgt om godkendelse af uddannelsen eller udbuddet?
Nej

Uddannelsestype
Master

Uddannelsens fagbetegnelse på dansk
Cybersikkerhed og risikohåndtering

Uddannelsens fagbetegnelse på engelsk
Cybersecurity and risk management

Angiv den officielle danske titel, som institutionen forventer at bruge til den nye uddannelse
Master i cybersikkerhed og risikohåndtering

Angiv den officielle engelske titel, som institutionen forventer at bruge til den nye uddannelse
Master of Cybersecurity and Risk Management

Hvilket hovedområde hører uddannelsen under?
Naturvidenskab

Hvilke adgangskrav gælder til uddannelsen?
Master i cybersikkerhed og risikohåndtering.

Følgende giver adgang til masteruddannelsen i cybersikkerhed og risikohåndtering:

En kandidat-, bachelor-, professionsbachelor- eller tilsvarende diplomuddannelse fra en videregående uddannelsesinstitution, der giver grundlæggende viden inden for mindst ét af følgende områder: datalogi, softwareudvikling, informationsteknologi, IT-arkitektur, erhvervsøkonomi, ledelse, økonomi eller organisationsstudier. For eksempel 10 ECTS-point fra kurser inden for programmering, computernetværk, operativsystemer, IT-sikkerhed eller databaseadministration, erhvervsledelse, organisationsudvikling, strategisk kommunikation eller offentlig forvaltning. Uddannelser inden for jura, kommunikation eller samfundsvidenskab kan også udgøre et tilstrækkeligt grundlag, hvis ansøgeren har gennemført relevante kurser inden for de nævnte kerneområder.

Ansøgerne skal have mindst to års relevant erhvervserfaring inden for mindst ét af følgende områder: softwareudvikling, IT-drift, IT-arkitektur, cybersikkerhed, systemadministration eller digital infrastruktur. Eller relevant erhvervserfaring i roller, der relaterer sig til organisatorisk styring eller digitale systemer, såsom data governance, IT-sikkerhed og compliance, IT-indkøb, regulatorisk compliance, projektledelse, risikostyring eller offentlig administration.

Er det et internationalt samarbejde, herunder Erasmus, fællesuddannelse el. lign.?
Nej

Hvis ja, hvilket samarbejde?

Hvilket sprog udbydes uddannelsen på?
Dansk

Er uddannelsen primært baseret på e-læring?
Nej, undervisningen foregår slet ikke eller i mindre grad på nettet.

ECTS-omfang
60

Beskrivelse af uddannelsens formål og erhvervssigte. Beskrivelsen må maks. fylde 1200 anslag

Formål: At efteruddanne nøglepersoner med ansvar inden for cybersikkerhed, risikostyring og forretningskontinuitet i små, mellemstore og store virksomheder, offentlige samt non-profit organisationer. Uddannelsen udstyrer nøglepersonerne med strategiske og operationelle kompetencer inden for IT-drift, cybersikkerhed, governance og digitale forsyningskæder, så de kan implementere cybersikkerhed og risikostyring i forretningsstrategier, der balancerer mellem tekniske muligheder, organisatoriske behov, juridiske rammer og interessentkrav. Dette er fundet relevant både regionalt og nationalt, som følge af behovsanalysen.

Erhvervssigte: At udstyre nøglepersoner med de nødvendige færdigheder til at påtage sig centrale roller inden for cybersikkerhedsindsatsen på tværs af alle brancher, der er afhængige af digitale systemer, f.eks. produktion, byggeri, sundhed, transport, finans, medier, IT og energi. Uanset om der er en høj eller lav grad af ekstern outsourcing af IT, er der et stigende behov for at styrke de interne kompetencer hos virksomheders nøglepersoner i overensstemmelse med den nationale strategi, europæiske forventninger samt den øgede efterspørgsel efter tværfaglig ekspertise.

Uddannelses struktur og konstituerende faglige elementer

I forbindelse med forskningsprojektet Cybersikkerhed og Forretningskontinuitet samarbejder Institut for Matematik og Datalogi ved Det Naturvidenskabelige Fakultet og Det Samfundsvidenskabelige Fakultet inden for områderne governance, forsyningsledelse og efterretning. Med afsæt i fælles forskning samt nye lovmæssige krav inden for cybersikkerhed og risikohåndtering møder de involverede forskere et stigende behov for at efter- og videreuddanne nøglepersoner inden for det digitale sikkerhedsområde med en ny kombination af kompetencer inden for cybersikkerhed og risikohåndtering i danske virksomheder regionalt og nationalt, dette for at kunne opretholde digital sikkerhed og dermed fortsat bevare høj konkurrenceevne.
Forskningsmiljøernes samarbejde med virksomheder bredt i Danmark har dannet grobund for denne uddannelse.

Uddannelsen leveres af institut for Matematik og Datalogi med støtte fra det Samfundsvidenskabelige Fakultet.

I nedenstående ses den overordnede uddannelsesopbygning:

Master i cybersikkerhed og risikohåndtering.
Uddannelsens struktur består af følgende elementer, 60 ECTS:

15 ECTS IT-systemer, softwareudvikling og strategisk organisering (afhængigt af ansøgerensbaggrund)
20 ECTS Virksomhedssikkerhed og risikostyring
10 ECTS Valgmoduler
15 ECTS Masteropgave

I det følgende uddybes uddannelsens struktur og faglige elementer, og uddannelsens konstituerede fagelementer er angivet med *:

1. semester:
Studerende med en uddannelsesbaggrund inden for IT-området (profil 1) skal vælge de to obligatoriske kurser inden for organisation. Studerende med en baggrund inden for det organisatoriske område (profil 2) skal vælge de to obligatoriske kurser inden for IT-systemer. De studerende kan derefter frit vælge det sidste kursus inden for enten IT-systemer eller organisation.
Dette semester har fokus på at opbygge et solidt fundament inden for både IT-systemer og organisation med henblik på at supplere den enkelte studerendes eksisterende baggrundsviden. Målet er at sikre, at alle studerende opnår en grundlæggende forståelse af både tekniske, ledelsesmæssige og organisatoriske aspekter, som er relevante for arbejdet med cybersikkerhed og risikohåndtering.

Profil 1 og 2 kan tage kurserne på 1. semester som isolerede forløb. Kurserne er tilstrækkeligt selvstændige og tilgængelige for studerende med den relevante generelle baggrund.

IT-systemer:
5 ECTS, Introduktion til Programmering og IT-systemer:
Dette kursus giver en praktisk introduktion til centrale komponenter i relevante IT-systemer og er målrettet studerende med begrænset eller ingen tidligere erfaring med programmering og systemværktøjer på operativt systemniveau. Kurset starter med grundlæggende programmering, herunder variabler, kontrolstrukturer, funktioner og basale datastrukturer, ved brug af et højniveaus programmeringssprog som f.eks. Python. De studerende får erfaring med at skrive og fejlrette enkle scripts, der er relevante for opgaver inden for cybersikkerhed og automatisering.
Parallelt introduceres brugen af command-line interface (CLI) i Unix-baserede systemer, med fokus på centrale operationer såsom navigation i filsystemer, fil- og proceshåndtering, rettigheder samt anvendelse af kommandolinjeværktøjer til automatisering og systeminspektion. Der lægges vægt på praktiske øvelser og virkelighedsnære scenarier, især relateret til systemadministration og incident response. De studerende arbejder også med grundlæggende databasekoncepter og relationelle databaser. Dette inkluderer at skrive enkle SQL-forespørgsler til at hente, opdatere og administrere data. Disse kompetencer er essentielle for at forstå logsystemer, revisionsspor og dataanalyse i en sikkerhedsmæssig kontekst.

Efter gennemført kursus vil den studerende kunne:
Skrive simple programmer og scripts til at automatisere opgaver eller udføre databehandling relateret til cybersikkerhed.
Anvende kommandolinjen effektivt til navigation i systemer, håndtere filer og processer samt basal fejlfinding.
Forstå og forklare CLI'ens og scriptingens rolle ved håndtering af sikkerhed i IT-systemer.
Bruge SQL til at forespørge og manipulere data i relationelle databaser.
Forbinde programmering, systemværktøjer og databaser i enkle arbejdsgange, der understøtter drifts- og sikkerhedsbehov.
Udvise øget digital dannelse og tryghed i mødet med tekniske IT-systemer, uanset tidligere erfaring.

Indhold i nøgleord: Digitale systemer. Programmering. Systemadministration. Arbejdsgange og automatisering af opgaver.

5 ECTS, Principper for Cybersikkerhed*:
Dette kursus giver en introduktion til de grundlæggende principper, der guider sikker systemdesign og -drift. Kurset henvender sig til studerende med forskellige baggrunde og har til formål at etablere en fælles forståelse af centrale begreber og terminologi inden for cybersikkerhed.
De studerende introduceres til væsentlige begreber som confidentiality, integrity og availability (CIA-triaden), samt til designprincipper såsom least privilege, minimal exposure, compartmentalisation og open design. Disse belyses gennem enkle eksempler og typiske scenarier fra alment anvendte digitale systemer, såsom brugerautentificering, filadgang og softwareinstallation. Dette er for at lære de studerende at håndtere anvendelsen af principperne i praksis.
I stedet for at fokusere på teknisk implementering eller formelle governance-rammeværk lægger kurset vægt på, hvorfor grundlæggende sikkerhedstænkning er vigtig. Herunder hvilke risici systemer er udsat for, hvorfor nogle arkitekturer er mere robuste end andre, og hvordan et godt design kan reducere sårbarheder. Kurset faciliterer de studerende til at tænke kritisk over balancen mellem brugervenlighed og sikkerhed og introducerer dem til det grundlæggende sprogbrug om risiko og forebyggelse, som videreudvikles i senere semestre.

Efter gennemført kursus vil de studerende kunne:
Beskrive de grundlæggende mål og principper for cybersikkerhed i både tekniske og ikke-tekniske sammenhænge.
Identificere, hvordan centrale sikkerhedsprincipper anvendes i enkle systemer og daglige IT-miljøer.
Genkende almindelige sikkerhedssvagheder, der opstår ved tilsidesættelse af grundlæggende designprincipper.
Udvise grundlæggende sikkerhedsbevidsthed om sikkerhedsrisici og kunne forklare, hvorfor visse sikkerhedsforanstaltninger er vigtige.
Anvende passende terminologi til at beskrive sikkerhedsrelaterede problemstillinger og formidle dem i en organisation, særligt til ikke-tekniske roller.

Indhold i nøgleord: Cybersikkerhed. Sikkerhedsbevidsthed. Databeskyttelse. Risikostyring. Interessentinddragelse. Kommunikation af risici.

5 ECTS, Computer Netværk og Cloud Computing*:
Dette kursus introducerer de studerende til de grundlæggende begreber inden for computernetværk og cloud computing, som er to kerneelementer i nutidens digitale infrastruktur. Kurset er designet til studerende uden en stærk teknisk baggrund og giver en praktisk og overordnet forståelse af, hvordan data bevæger sig gennem netværk, og hvordan cloud-tjenester anvendes til at levere skalerbare og robuste IT-løsninger.
De studerende starter med det basale inden for computernetværk, herunder hvad netværk er, hvordan enheder kommunikerer, og nøglebegreber såsom IP-adresser, protokoller og internettets struktur. Dette inkluderer en introduktion til klient-server-modellen, lokalnetværk (LAN), routing, firewalls og grundlæggende sikkerhedsovervejelser såsom kryptering og autentificering under dataoverførsel.
Anden del af kurset fokuserer på cloud computing. De studerende lærer, hvad cloud er, hvordan det adskiller sig fra traditionel lokal infrastruktur, og de centrale servicemodeller (IaaS, PaaS, SaaS). Kurset introducerer også almindelige anvendelser af cloudplatforme i både private virksomheder og offentlige organisationer, herunder datalagring, fjernadgang og skalerbarhed. I stedet for at fokusere på specifikke leverandørteknologier lægges vægten på begreber, praktiske implikationer og risici.
Gennem hele kurset anvendes virkelighedsnære eksempler for at lære de studerende at forstå, hvordan netværk og cloud-tjenester udgør fundamentet for alt fra fildeling på arbejdspladsen til netbank, og hvordan disse teknologier relaterer sig til cybersikkerhed og risikostyring.

Efter gennemført kursus vil de studerende kunne:
Beskrive de grundlæggende komponenter og funktioner i computernetværk, herunder centrale begreber som IP, DNS, protokoller og firewalls.
Forklare de grundlæggende principper og modeller for cloud computing samt identificere almindelige cloud-baserede tjenester og deres anvendelsesområder i praksis.
Forstå netværks- og cloudinfrastrukturens rolle i at muliggøre digitale tjenester på tværs af sektorer.
Identificere grundlæggende sikkerheds- og driftsmæssige bekymringer i netværks- og cloudmiljøer samt genkende typiske risikofaktorer.
Anvende denne forståelse til at vurdere IT-infrastrukturer på et overordnet niveau og deltage i kvalificeret dialog med tekniske specialister.

Indhold i nøgleord: Digital infrastruktur. Digitale tjenester. Cloud-sikkerhed og databeskyttelse.

Organisation:

5 ECTS, Introduktion til strategisk organisering og planlægning:

Dette kursus giver en bred introduktion til, hvordan organisationer fungerer, og hvordan strategiske beslutninger træffes i virksomheder og offentlige organisationer. Kurset henvender sig særligt til studerende med en teknisk baggrund og har fokus på at gøre dem fortrolige med centrale begreber inden for organisationsteori, ledelse og strategisk planlægning.
De studerende vil undersøge forskellige typer organisationsstrukturer (f.eks. hierarkiske, matrixbaserede, netværksbaserede), deres fordele og begrænsninger, samt hvordan disse strukturer påvirker beslutningstagning, kommunikation og ansvar. Kurset introducerer også grundlæggende modeller for strategisk ledelse, såsom SWOT-analyse og målorienteret planlægning. Dette for at give de studerende forståelse for, hvordan organisationer fastlægger langsigtede mål, fordeler ressourcer og tilpasser sig forandringer. Kurset fokuserer også på ledelsens rolle, organisationskulturen og interessenthåndteringen og giver indsigt i, hvordan organisatoriske mål omsættes til praksis. Hvor tekniske løsninger ofte fokuserer på, hvad der teknisk er mulig, lægger dette kursus vægt på, hvordan og hvorfor beslutninger træffes på det strategiske niveau, en viden, der er afgørende for at kunne integrere cybersikkerhed og risikostyring i bredere organisatoriske prioriteringer.

Efter gennemført kursus vil de studerende kunne:
Forstå centrale begreber inden for organisationsstruktur, roller og ledelse.
Beskrive, hvordan strategisk planlægning gennemføres, og hvordan mål tilpasses organisationens overordnede mission.
Genkende ledelsens og kommunikationens rolle i forandringsprocesser og risikohåndtering.
Indgå i dialog med ikke-tekniske interessenter på en måde, der understøtter sammenhæng mellem sikkerhedsmål og organisatorisk strategi.

Indhold i nøgleord: Strategisk sammenhæng. Interessentinddragelse. Organisationsstrukturer. Ledelse og kommunikation.

5 ECTS, Optimering af forretningsprocesser*:

Dette kursus introducerer de studerende til analyse og forbedring af forretningsprocesser, herunder de strukturerede aktiviteter, der skaber værdi i organisationer. Kurset giver tekniske fagpersoner de nødvendige værktøjer og det rette tankesæt til at identificere ineffektivitet, reducere risikovurdering og forbedre organisatorisk performance.
De studerende lærer at modellere og analysere processer ved hjælp af standardmetoder såsom flowcharts, proceskort og nøglepræstationsindikatorer (KPI'er). Desuden centrale begreber som flaskehalse, gennemløbstid, kapacitet og kontinuerlig forbedring, som inddrages gennem praktisk anvendelse. Kurset fokuserer også på, at procesoptimering ikke kun handler om effektivitet, men også om pålidelighed, robusthed og ansvarlighed, som er temaer, der er særdeles relevante i forhold til håndtering af cybersikkerhedsrisici og sikring af forretningskontinuitet. Gennem case-baserede øvelser lærer de studerende, hvordan IT-systemer enten understøtter eller hæmmer effektive processer, og hvordan digitalisering skaber både nye muligheder og sårbarheder.

Efter gennemført kursus vil de studerende kunne:
Forstå og beskrive centrale principper inden for Business Process Management (BPM).
Analysere og modellere enkle forretningsprocesser for at identificere ineffektivitet eller sårbarheder.
Anvende grundlæggende metoder til at forbedre processer med henblik på øget pålidelighed og reduceret risiko.
Koble procesforbedringer til bredere organisatoriske mål og krav om efterlevelse (compliance).

Indhold i nøgleord: Operationel risiko. Arbejdsgange. Effektivitet og pålidelighed. Procesanalyse.

5 ECTS, Resiliens i forsyningskæden*:
Dette kursus introducerer de studerende til den afgørende betydning af resiliens i forsyningskæder, herunder de sammenhængende netværk af leverandører, partnere og logistik, der gør det muligt for organisationer at fungere. Med den stigende digitalisering er forsyningskæder blevet mere effektive, men også mere sårbare over for forstyrrelser såsom cyberangreb, naturkatastrofer, lovgivningsmæssige ændringer samt geopolitiske begivenheder.
De studerende lærer om den grundlæggende struktur i forsyningskæder samt de strategiske beslutninger, der knytter sig til indkøb, lagerstyring, logistik og leverandørrelationer. Der lægges vægt på at identificere sårbarheder og udvikle strategier til risikominimering, diversificering og hurtig genopretning. Der anvendes virkelighedsnære cases, både fysiske og digitale, til at illustrere, hvordan fejl i forsyningskæden kan påvirke forretningskontinuitet og virksomhedens omdømme. De studerende får også en første introduktion til rammeværk for risikovurdering af forsyningskæder, en viden, der uddybes i senere semestre.

Efter gennemført kursus vil de studerende kunne:
Forstå strukturen og funktionen af forsyningskæder i både fysiske og digitale sammenhænge.
Genkende almindelige typer forstyrrelser og deres indvirkning på organisatoriske processer.
Identificere grundlæggende strategier til at styrke forsyningskædens resiliens og sikre kontinuitet.
Identificere IT's og datas rolle i overvågning, sikring og optimering af forsyningskæder.

Indhold i nøgleord: Operationel robusthed. Risikostyring. Forsyningskædestyring. Forretningskontinuitet. Analyse og overvågning af forsyningskæder.

2. semester:
På dette semester bygges der videre på den grundlæggende læring fra første semester. De studerende tillærer sig de kernekompetencer, der er nødvendige for at analysere og mindske risici i virksomhedssammenhæng, herunder læring om sikkerhedsstandarder, regulativer og governance-rammer, der er essentielle for at udvikle og implementere omfattende sikkerhedsarkitekturer. Fokus er på at udstyre de studerende med de færdigheder, der er nødvendige for at håndtere cybertrusler og sikre forretningskontinuitet.

Profil 1 og 2 kan tage kurserne på 2. semester isoleret, hvis de specifikke anbefalinger til de enkelte kurser opfyldes. Dette er nærmere beskrevet under hver kursusbeskrivelse nedenfor, under individuelle kursusforudsætninger.

7,5 ECTS, Trusselmodellering og risikostyring*:
Dette kursus giver de studerende centrale analytiske værktøjer og praktiske metoder til at identificere, vurdere og håndtere trusler og risici i organisatoriske sammenhænge. Med afsæt i de grundprincipper, der er introduceret i første semester, styrkes de studerendes evne til at tænke systematisk om både tekniske og organisatoriske trusler og til at anvende strukturerede tilgange til at imødegå dem.
De studerende introduceres til en række metoder til trusselmodellering, herunder STRIDE, angrebstræer og scenariebaserede risikovurderinger. Der arbejdes med, hvordan forskellige aktiver, systemer og aktører skaber forskellige risikobilleder, og hvordan sandsynlighed og konsekvens af trusler kan vurderes. Kurset dækker desuden de grundlæggende elementer i risikostyring, herunder identifikation, vurdering, planlægning af afhjælpning og risikokommunikation. Der lægges særlig vægt på balancen mellem tekniske løsninger og forretningsstrategiske behov, så sikkerhedsbeslutninger understøtter organisationens overordnede prioriteringer og ressourcer.

Efter gennemført kursus vil de studerende kunne:
Identificere og analysere cybertrusler ved brug af strukturerede modeller.
Gennemføre systematiske risikovurderinger, der tager højde for både tekniske og organisatoriske forhold.
Udvikle handlingsrettede planer for risikominimering, herunder prioritering af tiltag og vurdering af rest-risiko.
Formidle risici og anbefalinger klart til forskellige målgrupper med varierende teknisk baggrund.
Integrere trussel- og risikovurdering i strategisk planlægning og forretningskontinuitet.

Indhold i nøgleord: Risikostyring. Interessentinddragelse. Strategisk sammenhæng. Trusselmodellering. Fremtidstænkning. Operationel robusthed.

Individuelle kursusforudsætninger: Studerende, der tager dette kursus som et enkeltstående kursus, bør være fortrolige med grundlæggende cybersikkerhedsprincipper, digitale systemer og infrastruktur, basal risikobevidsthed, organisatoriske strukturer og strategisk tilpasning. Disse kompetencer kan erhverves ved at gennemføre relevante kurser fra første semester.
Til profil 1, anbefales det, at man er fortrolig med centrale begreber inden for strategisk planlægning, organisatoriske strukturer og procesmodellering, især i forhold til, hvordan risici og målsætning håndteres i en organisation.
Til profil 2, anbefales det, at man er fortrolig med grundlæggende digitale koncepter, IT-systemstrukturer og fundamentale cybersikkerheds-principper.

7,5 ECTS, Virksomhedens sikkerhedsarkitektur*:
Dette kursus introducerer de studerende til udvikling og implementering af sikkerhedsstrategier på virksomhedsniveau, og til hvordan tekniske kontroller kobles med governance, compliance og forretningsmål. Kurset har til formål at udstyre de studerende med værktøjer til at opbygge og evaluere sikkerhedsarkitekturer, der både overholder lovgivning og understøtter risikostyring.
De studerende arbejder med centrale standarder og rammeværk inden for cybersikkerhed, såsom ISO/IEC 27001, NIS2, CIS Controls og COBIT, og lærer, hvordan disse fortolkes og anvendes i forskellige organisatoriske kontekster. Der fokuseres på at omsætte krav til konkrete arkitekturer og procedurer, tilpasset organisationens risikoprofil, struktur og branche. De studerende vil arbejde med eksempler på arkitekturdokumentation, sikkerhedsblueprints og compliance-kortlægning.

Efter gennemført kursus vil de studerende kunne:
Forstå og sammenligne centrale rammeværk og standarder for cybersikkerhed.
Analysere, hvordan regulativer (fx NIS2) påvirker sikkerhedsplanlægning og -drift.
Udvikle og evaluere sikkerhedsarkitekturer, der er tilpasset både teknisk infrastruktur og forretningsmål.
Kortlægge kontroller og krav i forhold til organisationens risikobillede og compliance-behov.
Kommunikere strukturen og begrundelserne bag sikkerhedsarkitekturen til både tekniske teams og ledelse.

Indhold i nøgleord: Sikkerhedsarkitektur. Sikkerhedsdesign. IT-governance. Regulatorisk strategi. Interessentinddragelse. Strategisk sammenhæng. Compliance-rammeværk. Kommunikation. Implementering af kontroller og strategisk tilpasning.

Individuelle kursusforudsætninger: Studerende, der tager dette kursus som et enkeltstående kursus, bør have en grundlæggende forståelse af IT-systemer og organisatorisk planlægning samt være fortrolige med cybersikkerheds-principper samt organisatoriske strukturer. Kurset forbinder teknisk infrastruktur med strategisk styring, og de nødvendige kompetencer kan erhverves gennem kurser på første semester.
Til profil 1, anbefales det, at man er blevet introduceret til organisatoriske strukturer, ledelsesdynamikker og strategiske planlægningsmetoder, især i forhold til at tilpasse IT-systemer med forretningsmål.
Til profil 2, anbefales det, at man er fortrolig med nøglekomponenter i digital infrastruktur, systemniveau-tænkning og hvordan grundlæggende sikkerhedsprincipper anvendes i praksis.

3. semester:
Dette semester lægger vægt på praktisk anvendelse og specialisering. De studerende vil deltage i et feltstudie med det formål at observere og analysere reelle praksisser inden for cybersikkerhed. Derudover kan de studerende vælge blandt en række valgmoduler, der giver mulighed for at uddybe deres viden inden for specifikke interesseområder samt målrette deres viden til behovet i deres virksomhed, hvilket forbereder dem til specialiserede roller inden for cybersikkerhed og risikostyring.

Profil 1 og 2 kan tage kurserne på 3. semester isoleret (fraset feltstudiet), hvis de specifikke anbefalinger til de enkelte kurser opfyldes. Dette er nærmere beskrevet under hver kursusbeskrivelse nedenfor, under individuelle kursusforudsætninger.

5 ECTS, Feltstudie*:
Dette kursus giver studerende en unik mulighed for at observere og reflektere over virkelige cybersikkerheds- og risikostyringspraksisser i industrien, myndigheder eller i nonprofitorganisationer. Det vil foregå gennem planlagte besøg, interviews og observationer, hvor de studerende er i direkte kontakt med fagfolk, der er ansvarlige for digital sikkerhed og forretningskontinuitet.
De studerende skal analysere den praktiske implementering af risikostyringsstrategier, observere organisatoriske beslutningsprocesser samt identificere, hvordan sikkerhedspolitikker, teknologier og kommunikationspraksisser anvendes i forskellige kontekster. Kurset lægger vægt på at forbinde teoretisk viden fra de foregående semestre med faktisk organisatorisk adfærd, infrastruktur og begrænsninger. Kurset afsluttes med en refleksionsrapport, hvor de studerende evaluerer observationerne fra praksis og vurderer disse i overensstemmelse med bedste praksis samt med forslag til forbedringer eller alternative tilgange baseret på læringen opnået under uddannelsen.

Efter gennemført kursus vil de studerende kunne:
Observere og kritisk vurdere implementeringen af cybersikkerhed og risikostyring i virkelige organisatoriske sammenhænge.
Identificere mangler, styrker og muligheder i eksisterende praksis.
Forbinde teoretiske rammer med praktiske observationer.
Kommunikere indsigter klart til både tekniske og ikke-tekniske målgrupper.
Reflektere over de kulturelle, strukturelle og ressourcebaserede udfordringer ved anvendelse af sikkerhedsstrategier.

Indhold i nøgleord: Cybersikkerhedsarkitektur. Risikostyring. Strategisk tilpasning. Interessentinddragelse. Sikkerhed og ledelse i kontekst. Feltobservation. Kommunikation af risici.

10 ECTS, Valgmodul: De studerende skal vælge 10 ECTS fra følgende kurser:

5 ECTS, Intelligence og fremsynethed:
Dette kursus introducerer de studerende til brugen af efterretnings- og fremtidsforskningsmetoder inden for cybersikkerhed og organisatorisk risikostyring. De studerende lærer, hvordan organisationer indsamler og bruger data fra interne systemer, eksterne trusselsfeeds, brancherapporter og miljøscanning til at forudse risici og nye udfordringer.
Kurset dækker grundlæggende teknikker til horisontscanning, tidlige varslingssystemer og scenarieplanlægning, dette med fokus på at afdække komplekse og usikre digitale miljøer. Der vil blive anvendt virkelighedsnære øvelser og casestudier, så de studerende kan udvikle færdigheder til at omdanne rå information til handling. Kurset lægger vægt på, hvordan efterretning understøtter risikobaseret planlægning, strategisk tilpasning og kommunikation med interessenter på alle niveauer.

Efter gennemført kursus vil de studerende kunne:
Forstå efterretningens rolle inden for cybersikkerhed og strategisk risikostyring.
Anvende grundlæggende fremtidsforskning og analyseteknikker til at forudse fremtidige udfordringer.
Fortolke information fra interne og eksterne kilder for at forudse fremtidige risici.
Støtte proaktiv beslutningstagning baseret på analytisk ræsonnement.
Kommunikere efterretningsresultater klart og effektivt til anvendelse i strategisk planlægning og i politisk sammenhæng.

Indhold i nøgleord: Interessentengagement. Risikoforudsigelse. Strategisk fremtidsforskning. Tidlige varslingssystemer. Organisatorisk beslutningsstøtte.

Individuelle kursusforudsætninger: Studerende, der tager dette kursus som et selvstændigt modul, forventes at være fortrolige med grundlæggende principper inden for cybersikkerhed, virksomheders sikkerhedsarkitektur, organisationsstrukturer, trusselmodellering og risikostyring samt have et praktisk kendskab til digitale systemer og infrastruktur. Disse kompetencer kan opnås ved at gennemføre de relevante kurser på første studieår.

5 ECTS, Cyberspionage:
Dette kursus fokuserer på taktikker, værktøjer samt strategiske mål bag cyberspionage-aktiviteter. De studerende undersøger, hvordan statslige og ikke-statslige aktører gennemfører cyber-operationer med henblik på overvågning, tyveri af intellektuel ejendom eller for at opnå politisk indsigt og indflydelse. Der anvendes virkelighedsnære casestudier, som hjælper de studerende med at forstå, hvordan virksomheder og organisationer kan opdage, forhindre og reagere på spionagetrusler. Der lægges vægt på at forstå samspillet mellem geopolitik, cybersikkerhed og risikostyring.

Efter gennemført kursus vil de studerende kunne:
Beskrive cyberspionage og dens indvirkning på virksomheder og organisationer.
Analysere angrebsmønstre og indikatorer for spionageaktivitet.
Vurdere de forretningsmæssige og strategiske risici forbundet med informationslækage og målrettet overvågning.
Anbefale strategier til risikoreduktion.

Indhold i nøgleord: Bevidsthed om trusler. Risikostyring. Trusselsanalyse. Interne trusler. Informationstyveri. Geopolitisk risiko.

Individuelle kursusforudsætninger: Studerende, der tager dette kursus som et selvstændigt modul, forventes at være fortrolige med grundlæggende principper inden for cybersikkerhed, virksomheders sikkerhedsarkitektur, organisationsstrukturer, trusselmodellering og risikostyring samt at have et praktisk kendskab til digitale systemer og infrastruktur. Disse kompetencer kan opnås ved at gennemføre relevante kurser på første studieår.

5 ECTS, Etik og Privatliv:
Dette kursus fokuserer på de etiske og juridiske udfordringer, der opstår, når organisationer indsamler og behandler personfølsomme data i digitale systemer. Kurset fokuserer på de praktiske implikationer af privatliv og databeskyttelse inden for cybersikkerhed og IT-styring, og giver de studerende redskaber til at navigere i virkelige dilemmaer, hvor compliance, etik og forretningsmål mødes. Desuden introduceres vigtige lovgivningsmæssige rammer, såsom den generelle forordning om databeskyttelse (GDPR) og andre europæiske og sektorspecifikke standarder.

Efter gennemført kursus vil de studerende kunne:
Identificere centrale etiske og personfølsomme problemstillinger i design og drift af digitale systemer.
Forstå principperne og forpligtelserne relateret til databeskyttelsesregler.
Analysere og reagere på etiske dilemmaer inden for cybersikkerhed og datastyring.
Anvende bedste praksis for ansvarlig datastyring i organisatoriske sammenhænge.
Kommunikere begrundelser for datarelaterede beslutninger tilknyttet tekniske og ikke-tekniske interessenter.

Indhold i nøgleord: Sikkerhedsbevidsthed. Databeskyttelse. Datastyring. Privatlivsregulering. Compliance og ansvarlighed. Dataminimering. Informeret samtykke. Brugerautonomi og ansvarlighed i digitale infrastrukturer.

Individuelle kursusforudsætninger: Studerende, der tager dette kursus som et selvstændigt valgfag, forventes at være fortrolige med grundlæggende principper inden for cybersikkerhed, virksomheders sikkerhedsarkitektur og organisatoriske processer. Disse kompetencer kan opnås ved at gennemføre de relevante kurser i første studieår. Tidligere erfaring med datastyring og data governance er en fordel, men ikke et krav.

5 ECTS, Anvendt Cybersikkerhed:
Dette kursus er praktisk orienteret og introducerer de studerende til offensiv og defensiv cybersikkerhed gennem virkelighedsnære scenarier. De studerende lærer om cyber-angrebskæden, udnyttelse af sårbarheder og almindelige angrebsteknikker, hvor de anvender etiske hacking-metoder for at forstå, hvordan et hackerangreb fungerer. Der lægges vægt på at forbedre organisationens forsvar gennem indsigt i IT-systemers svagheder. De studerende vil arbejde med virkelige værktøjer i sikre miljøer.

Efter gennemført kursus vil de studerende kunne:
Beskrive livscyklus for et cyberangreb.
Identificere og forklare sårbarheder i IT-systemer.
Bruge etiske hackingværktøjer til at simulere og forstå angreb.
Foreslå tekniske og strategiske strategier til afbødning af angreb.

Indhold i nøgleord: Sikkerhedsbevidsthed. Defensive strategier. Etisk hacking. Cyber-angrebskæden.

Individuelle kursusforudsætninger: Studerende, der tager dette kursus som et selvstændigt modul, forventes at have solid forståelse for programmering, digitale systemer samt infrastruktur. Desuden at være fortrolige med grundlæggende principper inden for cybersikkerhed og virksomheders sikkerhedsarkitektur. Disse kompetencer kan opnås ved at gennemføre de relevante kurser på første studieår.

5 ECTS, Sikker Softwareoperation:
Dette kursus fokuserer på principperne og praksis bag sikker softwareudvikling og drift, med afsæt i DevSecOps. De studerende lærer, hvordan sikkerhed kan integreres i hele softwarens livscyklus, fra design og udvikling til implementering og vedligeholdelse.

Efter gennemført kursus vil de studerende kunne:
Beskrive sikkerhedens rolle i softwareudviklingens livscyklus.
Identificere bedste praksis for opbygning og implementering af sikker software.
Forstå DevSecOps-modellen og dens implikationer for virksomheder og organisationer.
Anbefale forbedringer af eksisterende softwarepipelines ud fra et sikkerhedsperspektiv.

Indhold i nøgleord: Digitale systemer og infrastruktur. Digitale arbejdsgange. Digital forsyningskæde. Softwarepipelines. Konfigurationsstyring. DevSecOps. Sikker kodningspraksis. Automatiseret test. Kontinuerlig integration og overvågning af sårbarheder.

Individuelle kursusforudsætninger: Studerende, der tager dette kursus som et selvstændigt modul, forventes at have en solid forståelse for programmering samt for digitale systemer og infrastruktur. Desuden skal de være fortrolige med grundlæggende principper inden for cybersikkerhed og virksomheders sikkerhedsarkitektur. Disse kompetencer kan opnås ved at gennemføre de relevante kurser på første studieår.

4. semester:

15 ECTS, Masteropgave:

Det sidste semester er dedikeret til masteropgaven, hvor de studerende gennemfører en selvstændig, dybdegående undersøgelse af et emne, der er relevant for cybersikkerhed og risikostyring. Opgaven kan tage form af enten en videnskabelig undersøgelse eller et praksisorienteret projekt, der er integreret i en organisation eller virksomhed, eventuelt den studerendes egen arbejdsplads.

De studerende identificerer et konkret problem, et forskningsspørgsmål eller en strategisk udfordring og anvender de teorier, metoder, værktøjer og kompetencer, de har tilegnet sig under uddannelsen, til at løse det. Emnerne kan spænde sig fra evaluering af sikkerhedsarkitekturer eller styringsmodeller til implementering af risikostyringsstrategier eller vurderinger af organisatorisk modenhed.

For masterprojekter, der gennemføres i samarbejde med virksomheder, forventes det, at de studerende udformer deres arbejde på en måde, der kombinerer faglig relevans med akademisk stringens, og de trækker på relevant litteratur, rammer og analyser.

Masteropgaven afsluttes med en skriftlig afhandling, der demonstrerer den studerendes evne til at arbejde selvstændigt, integrere tværfaglig viden og fremkomme med velbegrundede konklusioner eller anbefalinger.

Kompetenceprofil:

Masteruddannelsen i cybersikkerhed og risikostyring er designet til at uddanne nøglepersoner, der er ansvarlige for cybersikkerhed, risikostyring og forretningskontinuitet på tværs af sektorer, i små, mellemstore og store virksomheder, i offentlige institutioner og i nonprofit organisationer, med roller, der spænder over forretningsledere, IT-drift, compliance, indkøb og digital strategi. Dimittender fra uddannelsen vil opnå en stærk og alsidig kombination af strategisk indsigt, operationelle værktøjer og tværfaglig viden, der er nødvendig for at vurdere, implementere og lede indsatser inden for cybersikkerhed og risikostyring, der er i overensstemmelse med forretningsstrategi, lovgivningsmæssige krav samt digitale infrastrukturer og tjenester.

Ved afslutningen af uddannelsen vil dimittenderne være i stand til at:

Designe og evaluere sikkerhedsarkitekturer, der integrerer cyber-risici med bredere forretningsrisici og mål, og som understøtter operationel robusthed, regulatorisk overholdelse og konkurrenceevne.
Udvikle sikkerhedspolitikker og planer, herunder strategier for håndtering af hændelser, beredskab og genopretning, skræddersyet til deres teknologier, trusselslandskab og modenhedsniveau i deres virksomhed eller organisation.
Navigere og anvende store regulatoriske rammer og standarder (f.eks. ISO/IEC 27001, NIS2, GDPR) ved hjælp af etablerede værktøjer og metoder til vurdering og implementering.
Udføre strukturerede trussels- og risikovurderinger ved hjælp af brancheanerkendte modeller (f.eks. STRIDE og angrebstræer) for at informere til beslutningstagning på både teknisk og strategisk niveau samt oversætte resultaterne til handlingsorienterede strategier.
Styrke cybersikkerhedskultur og bevidsthed i deres virksomhed eller organisation ved at engagere ikke-tekniske kolleger, lede forandringsinitiativer og indføre gode sikkerhedspraksisser i daglige arbejdsprocesser.
Sikre governance-justering ved at integrere cybersikkerhed og risikoreduktion i forretningsplanlægning, forsyningskædestyring, digitaliseringsstrategier og IT-indkøbspraksis for at reducere sårbarheder og forbedre robusthed.
Anvende efterretningsmetoder og metoder til at forudse risici, forstå nye trusler og understøtte proaktiv beslutningstagning baseret på scenarieplanlægning og tidlige advarselssignaler, der kan forudse, mindske eller undgå forstyrrelser i virksomheden.
Lede effektivt i kriser og usikkerhed ved at anvende lederskab, kommunikation og interessentengagement i krisesituationer og i strategisk planlægning. Desuden understøtte tværfunktionelle initiativer, der øger sikkerhedsmodenhed og opretholder tillid og langsigtet kontinuitet.
Arbejde forebyggende med cybersikkerhed og risikostyring samt reducere eksponering før hændelser opstår ved at identificere sårbarheder, forbedre processer og fremme robusthed på tværs af digitale infrastrukturer og forsyningskæder.

Af praktiske værktøjer vil dimittenderne kunne:

Anvende skabeloner og modeller til sikkerhedsarkitektur og governance-styring.
Anvende rammeværktøjer til modellering af trusler og risici.
Anvende teknikker til procesmodellering og optimering.
Anvende værktøjer til overholdelse- og modenhedsvurdering.
Anvende kommunikations-strategier, særligt målrettet ikke-tekniske målgrupper.

Dimittenderne vil bidrage til brobygning mellem de tekniske og organisatoriske områder i en virksomhed inden for cybersikkerhed og risikohåndtering. Med kompetencer til at oversætte risici til strategiske prioriteringer og kommunikere på tværs af afdelinger og niveauer vil de spille en nøglerolle i at fremme virksomhedens eller organisationens modenhed inden for cybersikkerhed, den operationelle robusthed og virksomhedens langsigtede beredskab.

Begrundet forslag til takstindplacering af uddannelsen

Takstgruppe tre.

Forslag til censorkorps

Uddannelsen tilknyttet censorkorps for datalogi, med mulighed for at supplere inden for relevante felter hos censorkorps for erhvervsøkonomi.

Dokumentation af efterspørgsel på uddannelsesprofil - Upload PDF-fil på max 30 sider. Der kan kun uploades én fil

Final_Arbejdsmarkedsbehovsundersøgelsen_og_Følgebrev_Master_cybersikkerhed_og_risikoha■ndtering_2025.pdf

Kort redegørelse for det nationale og regionale behov for den nye uddannelse. Besvarelsen må maks. fylde 1800 anslag

Litteraturen, behovsundersøgelsen, nye regulatoriske krav samt en hyppigere og tiltagende grad af avancerede cybertrusler i virksomheder og organisationer fremhæver et aktuelt og stigende behov for nye kompetencer i virksomheder regionalt og nationalt. Denne uddannelse imødekommer disse krav og behov ved at udstyre nøglepersoner med ansvar for cybersikkerhed og risikohåndtering i små, mellemstore og store virksomheder, offentlige organisationer samt non-profit organisationer, med nye interdisciplinære kompetencer inden for cybersikkerhed, risikostyring og forretningskontinuitet, der er nødvendige for både at tage højde for operationelle behov og de bredere forsyningskæderisici og dermed sikre forretningens bestående.

Eksisterende efteruddannelser fokuserer enten på tekniske kompetencer inden for cybersikkerhed eller på forretningsledelse, og de integrerer ikke de to perspektiver i én uddannelse, som denne uddannelse gør. Uddannelsens formål kan således ikke opfyldes af eksisterende uddannelser.

I behovsanalysen og litteraturen blev det klart, at mange virksomheder har begrænsede ressourcer til at sikre sig digitalt. Desuden er rollen inden for cybersikkerhed og risikohåndtering ofte fordelt på flere personer med forskellige uddannelsesbaggrunde, og virksomhederne skal have et vist kompetenceniveau internt, uanset graden af tilkøb af eksterne ydelser til opgaveløsningen. Uddannelsen vil derfor også imødekomme arbejdsmarkedets behov ved at uddanne to profilretninger: Profil 1 med en IT-baggrund og profil 2 med anden baggrund og relevant erhvervserfaring. For at imødekomme realiteterne og behovene i virksomhederne, vil det være muligt at tage uddannelsen i form af enkelte fag eller semestre, løbende eller isoleret.

Uddybende bemærkninger

Ovenstående er baseret på følgende kilder:

National strategi for cyber- og informationssikkerhed 2022-2024:
https://fm.dk/media/rgmchosw/national-strategi-for-cyber-og-informationssikkerhed_web-a.pdf
Barometerundersøgelsen 2024:
https://itb.dk/nyheder/her-er-branchens-stoerste-vaekstbarrierer-for-2024/
https://docs.google.com/presentation/d/1wpByDFix11Nw1X5ENGbLQoqInLhC8CYl/edit?slide=id.p1#slide=id.p1.
Cybersikkerhed i små og mellemstore danske produktionsvirksomheder 2024:
https://findresearcher.sdu.dk/ws/portalfiles/portal/265031161/Cybersikkerhed_i_smaa_og_mellemstore_danske_produktionsvirksom
Digital sikkerhed i danske SMV'er 2024:
https://digst.dk/media/hskb5hdp/digital-sikkerhed-i-danske-smver-2023_endelig0310-a.pdf
Arbejdsmarkedsbehovsundersøgelsen (2025).

Underbygget skøn over det nationale og regionale behov for dimittender. Besvarelsen må maks. fylde 1200 anslag

Vi forventer at uddanne 10 dimittender på første forløb og derefter 15 årligt på den fulde uddannelse.
Vi forventer desuden at uddanne 20 studerende pr. semester, som enten tager ét eller to fag eller ét helt semester. Disse studerende vil følge undervisningen sammen med dimittender, der følger det fulde forløb. Det vil være muligt på 1. og 2. semester samt på valgfagene på 3. semester, under forudsætning af de samme optagelseskriterier samt yderligere specificeret relevant erfaring tilknyttet muligheden på 2. og 3. semester.

Efter den gennemførte behovsanalyse har aftagerne bredt set fremhævet et behov for fleksibilitet i måden at tage uddannelsen på. Institut for Matematik og Datalogi har valgt at imødekomme behovet ved, at nøglepersoner inden for cybersikkerhed og risikohåndtering kan tage enkelte fag eller semestre på uddannelsen isoleret eller med forløb, der strækker sig over to år.
Det samlede skøn er baseret på behovsanalysen fra 2025 og på interviews med beslutningstagere fra virksomheder i forbindelse med forskningsprojektet "Cybersikkerhed og Forretningskontinuitet", som tilsammen indikerer et stigende behov for at efteruddanne nøglepersoner inden for området.

Hvilke aftagere har været inddraget i behovsundersøgelsen? Besvarelsen må maks. fylde 1200 anslag

SDUs aftagerundersøgelse består af nøglepersoner og ledere fra virksomheder, organisationer, interesseorganisationer og ét erhvervshus på tværs af brancher, både regionalt og nationalt i Danmark:

Indledningsvist blev uddannelsen præsenteret på et styregruppemøde i Cybersikkerhed og Forretningskontinuitet i januar 2025 med repræsentanter fra: Dansk Industri (DI). DI2X – Digital Leadership Research Institute. KFISCH. Zoriac Aps. Fra SDU deltog Dekanen på Det Naturvidenskabelige Fakultet samt repræsentanter fra Institut for Matematik og Datalogi, Center for War Studies, Institut for Erhverv og Bæredygtighed samt Forsvarsakademiet.

Interviews blev foretaget i foråret 2025 med: Fire Eater. Terma. KFISCH, DIIS, Dansk Institut for Internationale Studier og Forsvarsministeriet. Dansk Gummi Industri. Gomspace. Rambøll. Sparrow Quantum. Digital Frontier. Orifarm. Odense Kommune. Jeros. Dansk Sintermetal. HMK Bilcon. Unik Systemdesign. Energinet. Bankdata.

Støtteerklæringer er indhentet fra:

KFISCH. Dansk Gummi Industri. Rambøll. Unik Systemdesign. Technology Denmark. Erhvervshus Fyn.

Der henvises desuden til arbejdsmarkedsbehovsundersøgelsen i medsendte bilag.

Hvordan er det konkret sikret, at den nye uddannelse matcher det påviste behov? Besvarelsen må maks. fylde 1200 anslag

Aftagerne ser et aktuelt og stigende behov for at efteruddanne inden for kombinationen af cybersikkerhed og risikohåndtering, regionalt og nationalt.

De fremhæver uddannelsens indhold og sammensætning som ambitiøst og relevant for nøglepersoner i virksomheder og organisationer.

Aftagerne anbefaler mere fleksibilitet i uddannelsen, hvilket vil gøre den endnu mere attraktiv. Forskningsmiljøet vil imødese dette ved at tilbyde mulighed for at tage dele af uddannelsen, ét fag eller ét semester, løbende eller isoleret.

De fremhæver også vigtigheden af en tydeligere profil med mere sammenhæng mellem adgangskriterier, målgruppe, kurser og formål. Forskningsmiljøet har præciseret dette i uddannelsen gennem profil 1 og 2.

Aftagerne anbefaler et nyt perspektiv i form af et vedvarende fagligt netværk. Forskningsmiljøet har iværksat udviklingen af dette i form af et hub, hvor forskere og virksomheder kan mødes om cybersikkerhed og risikohåndtering.

Endelig anbefaler aftagerne et øget fokus på formidlingen af gevinsten ved at gennemføre uddannelsen samt på uddannelsens praktiske aspekter. Forskningsmiljøet og ledelse er opmærksomme på at afsætte ressourcer til markedsføringsindsatsen.

Beskriv ligheder og forskelle til beslægtede uddannelser, herunder beskæftigelse og eventuel dimensionering. Besvarelsen må maks. fylde 1200 anslag

Master i cybersikkerhed og risikohåndtering, SDU:
Uddannelsen har et tværfagligt fokus, der kombinerer risikostyring inden for cybersikkerhed, IT-governance samt forretnings- og forsyningskædestyring, og giver nøglepersoner inden for cybersikkerhed, risikostyring og forretningskontinuitet mulighed for at udvikle omfattende sikkerhedsarkitekturer, der integrerer cyberrisici med forretningsrisici, som styrker digital sikkerhed. Uddannelsen er ikke direkte beslægtet med eksisterende uddannelser i Danmark.

Delvist beslægtede uddannelser (uddybes nedenfor):

Master in Intelligence and Cyber Studies (MICS), SDU.
Master in Cyber Security and Privacy, AAU.
Master of Cyber Security, DTU.
IT-sikkerhed, Diplomuddannelse, UCL.
Masteruddannelsen i IT-sikkerhed, IT-Vest.

Beskæftigelse: Der forventes et stigende behov for at efteruddanne nøglepersoner inden for cybersikkerhed og risikohåndtering i flertallet af virksomheder og organisationer til at varetage risikostyring og forbedre cybersikkerheden. Afsættet er en stigende grad af cybertrusler og øget regulatoriske krav, der kræver, at virksomheder udvikler robuste sikkerhedsarkitekturer.

Dimensionering: Ikke omfattet heraf.

Uddybende bemærkninger

Jf. ovenstående beskrives i følgende, delvist beslægtede uddannelser med et vist fagligt overlap:

Master in Intelligence and Cyber Studies (MICS), SDU:

Uddannelsen fokuserer på myndigheder, politi, forsvar, geopolitik og efterretning. Der er et vist fagligt overlap, da begge uddannelser underviser i færdigheder relateret til efterretning og analyse, men med forskellige anvendelsesfokus, geopolitik versus erhvervsliv. Dette overlap er begrænset til 10 ECTS.
Samfundsvidenskab er involveret i denne nye masteruddannelse, og de to fakulteter koordinerer for at undgå overlap.

Master in Cyber Security and Privacy, AAU:

Uddannelsen fokuserer på datalogi samt offensiv og defensiv sikkerhed. Derudover omfatter den også sikkerhed i softwareudvikling og systemadministration. Uddannelsen er målrettet udviklingen af specialister inden for cybersikkerhed, som kan arbejde i roller inden for softwareudvikling og rådgivning i store virksomheder. Der er et vist fagligt overlap, da begge uddannelser inkluderer aspekter af cybersikkerhed. Denne uddannelse indeholder ikke fokus på læring om integration af cybersikkerhed, risikostyring og forretningskontinuitet, og den udbydes på engelsk.

Master of Cyber Security, DTU:

Uddannelsen fokuserer på datalogi og software engineering, med specialisering i softwareudvikling samt IT-ledelse og administration. Den er en målrettet uddannelse af specialister inden for cybersikkerhed i store virksomheder samt i konsulentvirksomheder. Der er et vist fagligt overlap, idet begge uddannelser fokuserer på regler og standarder relateret til cybersikkerhed. Denne uddannelse har dog et begrænset fokus på forretningsaspekter og udbydes på engelsk.

IT-sikkerhed, Diplomuddannelse på UCL:

Uddannelsen fokuserer på de tekniske aspekter af IT-ledelse og softwareudvikling, men ikke på forretnings- og forsyningskæder. Uddannelsen er målrettet IT-professionelle (udviklere og systemadministratorer), der ønsker at forbedre deres færdigheder inden for cybersikkerhed. Der er et vist fagligt overlap, idet begge uddannelser dækker principperne inden for cybersikkerhed og relaterede standarder.

Masteruddannelsen i IT-sikkerhed, IT-Vest:

Uddannelsen har to profiler:
Profil 1 fokuserer på softwarekonstruktion og organisation, herunder de tekniske aspekter af IT-ledelse og softwareudvikling, men ikke på forretnings- og forsyningskædeaspekter. Der er vist fagligt overlap, idet profil 1 dækker principperne for cybersikkerhed og relaterede standarder.
Profil 2 fokuserer på organisation og IT-ledelse, men har et begrænset fokus på cybersikkerhed. Der er også her et vist fagligt overlap, idet studerende med profil 2 kan vælge kurser, der kombinerer grundlæggende IT-sikkerhed og virksomhedsledelse. Men selvom dette vælges, vil de ikke opnå samme specialiserede niveau mellem cybersikkerhed og forretningskontinuitet som på masteren i cybersikkerhed og risikohåndtering på SDU.
Både profil 1 og 2 er målrettet IT-professionelle (softwareudvikler og systemadministratorer), der ønsker at forbedre deres færdigheder inden for cybersikkerhed, mens masteruddannelsen i cybersikkerhed og risikohåndtering på SDU primært henvender sig bredt til nøglepersoner inden for cybersikkerhed, risikostyring og forretningskontinuitet i virksomheder og organisationer.

Beskriv rekrutteringsgrundlaget for ansøgte, herunder eventuelle konsekvenser for eksisterende beslægtede udbud. Besvarelsen må maks. fylde 1200 anslag

Uddannelsen forventes ikke at have en negativ indvirkning på rekrutteringsgrundlaget for relaterede uddannelser. I stedet komplementerer den eksisterende udbud ved at bidrage med en ny uddannelsesvej, der imødekommer den stigende efterspørgsel efter fagfolk, som kan bygge bro mellem teknologi og forretningsstrategi. Denne uddannelse vil tiltrække et andet segment af ansøgere, som er særligt interesseret i krydsfeltet mellem cybersikkerhed og forretningskontinuitet, hvilket udvider det samlede rekrutteringsgrundlag.

Det forventes at kunne rekruttere nøglepersoner regionalt og nationalt inden for cybersikkerhed, risikostyring og forretningskontinuitet fra små, mellemstore og store virksomheder, offentlige organisationer samt non-profit organisationer med en baggrund inden for grundlæggende datalogi, softwareudvikling, forretningsledelse eller økonomi, som ønsker at forbedre deres færdigheder inden for både cybersikkerhed og forretningskontinuitet.

I modsætning til eksisterende masteruddannelser fra AAU, DTU og UCL, der fokuserer på tekniske aspekter, kombinerer dette program cybersikkerhed med risikostyring inden for forretning og forsyningskæde.

Beskriv kort mulighederne for videreuddannelse

Ikke relevant.

Forventet optag på de første 3 år af uddannelsen. Besvarelsen må maks. fylde 200 anslag

Vi forventer at optage 10 dimittender det første år og derefter 15 pr. år på den fulde uddannelse, desuden at optage 20 studerende pr. semester, som tager ét eller to fag eller ét helt semester.

Hvis relevant: forventede praktikaftaler. Besvarelsen må maks. fylde 1200 anslag

Ikke relevant.

Øvrige bemærkninger til ansøgningen

Ingen øvrige bemærkninger.

Hermed erklæres, at ansøgning om prækvalifikation er godkendt af institutionens rektor

Ja

Status på ansøgningen

Godkendt

Ansøgningsrunde

2025-2

Afgørelsesbilag - Upload PDF-fil

Afgørelsesbrev A1 Masteruddannelse i cybersikkerhed og risikohåndtering, Odense.pdf

Samlet godkendelsesbrev - Upload PDF-fil

Bilag til prækvalifikationsansøgning for master i cybersikkerhed og risikohåndtering

Syddansk Universitet, Odense

September 2025

Udarbejdet af fuldmægtig Sabine Gantzhorn Hildebrand, sabh@sdu.dk.
Det Naturvidenskabelige Fakultetssekretariat, SDU.

Indhold

UDDANNELSENS INDHOLD OG OPBYGNING **3**

ANDRE MASTERUDDANNELSER INDEN FOR CYBERSIKKERHED OG RISIKOHÅNDTERING **4**

BEHOVSUNDERSØGELSE **6**

RESUME **7**

KONKLUSION – EVIDENSEN INDEN FOR CYBERSIKKERHED OG RISIKOHÅNDTERING 7
KONKLUSION – AFTAGERNES PERSPEKTIVER PÅ MASTERUDDANNELSEN 8
ANBEFALINGER OG POINTER FRA SDU'S AFTAGERUNDERSØGELSE 9
REVISION AF UDDANNELSENS INDHOLD EFTER AFTAGERNES ANBEFALINGER 9

METODE **12**

EVIDENS 12
AFTAGER 15
1. Behovet for masteruddannelse inden for cybersikkerhed og risikohåndtering *17*
DELKONKLUSION OM BEHOVET FOR EN MASTER I CYBERSIKKERHED OG RISIKOHÅNDTERING PÅ SDU 20
2. Uddannelsens indhold og sammensætning *21*
DELKONKLUSION OM HVILKE KOMPETENCER AFTAGERNE FREMHÆVER BØR STYRKES ELLER ER SÆRLIGT VIGTIGE 23
DELKONKLUSION OM HVILKE NYE PERSPEKTIVER AFTAGERNE MENER VIL TILFØRE MERE VÆRDI TIL UDDANNELSEN 24
DELKONKLUSION OM HVILKE ANDRE PERSPEKTIVER SDU BØR VÆRE OPMÆRKSOMME PÅ 25

STØTTEERKLÆRINGER **26**

REFERENCER **27**

Uddannelsens indhold og opbygning

Kassogram:

1.semester	(I alt 15 ECTS #)	
	IT-Systemer. - **Introduktion til relevante IT-systemer.** - **Principper for Cybersikkerhed*.** - **Computer Netværk og Cloud Computing*.**	**Organisation.** - **Introduktion til strategisk organisering og planlægning.** - **Optimering af forretningsprocesser*.** - **Resiliens i forsyningskæden*.**
2.semester	(7,5 ECTS) **Forbedret trusselmodellering og risikostyring*.**	(7,5 ECTS) **Virksomhedens sikkerhedsarkitektur*.**
3.semester	(5 ECTS) **Feltstudie*.**	(10 ECTS ##) **Valgmodul:** - **Intelligence og fremsynethed** - **Cyberspionage** - **Etik og Privatliv** - **Anvendt Cybersikkerhed**
4.semester	(15 ECTS) **Masteropgave.**	

(#) Uddybende beskrivelse til første semester. Den studerende skal i alt vælge tre kurser, 15 ECTS. Studerende med en uddannelsesbaggrund inden for IT-området (*profil 1*) skal vælge de to obligatoriske kurser inden for **organisation**. Studerende med en baggrund inden for det organisatoriske område (*profil 2*) skal vælge de to obligatoriske kurser inden for **IT-systemer**. De studerende kan derefter frit vælge det sidste kursus inden for enten IT-systemer eller organisation.
Dette semester har fokus på at opbygge et solidt fundament inden for både IT-systemer og organisation med henblik på at supplere den enkelte studerendes eksisterende baggrundsviden. Målet er at sikre, at alle studerende opnår en grundlæggende forståelse af både tekniske, ledelsesmæssige og organisatoriske aspekter, som er relevante for arbejdet med cybersikkerhed og risikohåndtering.

(##) Uddybende beskrivelse til 3. semester. Den studerende kan i alt vælge 10 ECTS, svarende til to ud af de fire valgmuligheder, og dermed tone retningen på deres profil.

Det vil være muligt at tage uddannelsen fleksibelt. Hermed menes, at alle moduler på første og andet semester samt valgmodulerne på tredje semester kan tilbydes som selvstændige kurser. Modulerne er tilstrækkeligt selvstændige og tilgængelige for studerende med det rette erfaringsgrundlag. Dette giver både studerende og arbejdsgivere mulighed for at målrette opkvalificering uden at skulle forpligte sig til det fulde uddannelsesforløb fra start.

Andre masteruddannelser inden for cybersikkerhed og risikohåndtering

Listen nedenfor viser andre danske lignende masteruddannelser inden for cybersikkerhed og risikohåndtering.

Master på SDU. ***Master in Intelligence and Cyber Studies (MICS)***	Uddannelsen fokuserer på myndigheder, politi, forsvar, geopolitik og efterretning. Der er et vist fagligt overlap, da begge uddannelser underviser i færdigheder relateret til efterretning og analyse, men med forskellige anvendelsesfokus, geopolitik versus erhvervsliv. Dette overlap er begrænset til 10 ECTS. Samfundsvidenskab er involveret i denne nye masteruddannelse, og de to fakulteter koordinerer for at undgå overlap.
Master på AAU. ***Master in Cyber Security and Privacy***	Uddannelsen fokuserer på datalogi samt offensiv og defensiv sikkerhed. Derudover omfatter den også sikkerhed i softwareudvikling og systemadministration. Uddannelsen er målrettet udviklingen af specialister inden for cybersikkerhed, som kan arbejde i roller inden for softwareudvikling og rådgivning i store virksomheder. Der er et vist fagligt overlap, da begge uddannelser inkluderer aspekter af cybersikkerhed. Denne uddannelse indeholder ikke fokus på læring om integration af cybersikkerhed, risikostyring og forretningskontinuitet, og den udbydes på engelsk.
Master på DTU. ***Master of Cyber Security***	Uddannelsen fokuserer på datalogi og software engineering, med specialisering i softwareudvikling samt IT-ledelse og administration. Den er en målrettet uddannelse af specialister inden for cybersikkerhed i store virksomheder samt i konsulentvirksomheder. Der er et vist fagligt overlap, idet begge uddannelser fokuserer på regler og standarder relateret til cybersikkerhed. Denne uddannelse har et begrænset fokus på forretningsaspekter og udbydes på engelsk.
Master ved IT-Vest. ***Masteruddannelsen i IT-sikkerhed***	Uddannelsen har to profiler: Profil 1 fokuserer på softwarekonstruktion og organisation, herunder de tekniske aspekter af IT-ledelse og softwareudvikling, men ikke på forretnings- og forsyningskædeaspekter. Der er vist fagligt overlap, idet profil 1 dækker principperne for cybersikkerhed og relaterede standarder. Profil 2 fokuserer på organisation og IT-ledelse, men har et begrænset fokus på cybersikkerhed. Der er også her et vist fagligt overlap, idet studerende med profil 2 kan vælge kurser, der kombinerer grundlæggende IT-sikkerhed og virksomhedsledelse. Men selvom dette vælges, vil de ikke opnå samme specialiserede niveau mellem cybersikkerhed og forretningskontinuitet som på masteren i cybersikkerhed og risikohåndtering på SDU. Både profil 1 og 2 er målrettet IT-professionelle (softwareudvikler og systemadministratorer), der ønsker at forbedre deres

	færdigheder inden for cybersikkerhed, mens masteruddannelsen i cybersikkerhed og risikohåndtering på SDU primært henvender sig bredt til nøglepersoner inden for cybersikkerhed, risikostyring og forretningskontinuitet i virksomheder og organisationer.

Behovsundersøgelse

Denne arbejdsmarkedsbehovsundersøgelse består af:

1.) National strategi for cyber- og informationssikkerhed 2022-2024 (1).

2.) Barometerundersøgelsen 2024 (2).

3.) Cybersikkerhed i små og mellemstore danske produktionsvirksomheder 2024 (3).

4.) Digital sikkerhed i danske SMV'er 2024 (4).

5.) SDU's aftagerundersøgelse (2025).

6.) Støtteerklæringer fra relevante aftagere (2025).

Ovenstående skal belyse, at der er samfundsmæssig relevans og et behov for efter- og videreuddannelse inden for cybersikkerhed og risikohåndtering både regionalt og nationalt.

Resume

Konklusion – evidensen inden for cybersikkerhed og risikohåndtering

I den nationale strategi for cyber- og informationssikkerhed 2022-2024[1] fremhæves en mangel på kompetencer og et behov for mere uddannelse inden for området cybersikkerhed og risikohåndtering. Dette anses for nødvendigt, hvis Danmark skal kunne bevare sin digitaliseringskraft og være på forkant med udviklingen i cybertrusler og digitale sårbarheder. Den høje grad af digitalisering medfører nemlig en øget sårbarhed over for kriminelle, der forsøger at udnytte det digitale samfund. Truslen fra cyberkriminalitet og cyberspionage er i dag meget høj, og det forventes at forblive sådan i fremtiden. Derfor betragter regeringen cybertruslen som en af de mest alvorlige trusler mod Danmark. Dette stiller høje krav til, hvordan samfundet håndterer beskyttelsesværdige informationer og den digitale infrastruktur. Samtidigt stilles der også krav fra EU om at højne cybersikkerheden.

I Danmark er der høj efterspørgsel på kompetencer inden for cyber- og informationssikkerhed, og både myndigheder og virksomheder har svært ved at skaffe de rette profiler til opgaverne. Det fremhæves, at der er et behov for at styrke udbuddet af kompetencer, hvis sikkerheden skal løftes bredt set. Derfor er en del af den strategiske løsning mod et stærkere og mere sikkert digitalt Danmark, at virksomheder og organisationer opkvalificeres med nye kompetencer inden for cyber- og informationssikkerhed.

I IT-branchens årlige brancheanalyse fra 2024[2] fremhæves det, at manglen på it-kompetencer er den absolut største barriere for vækst i IT-branchen. 40% af virksomhederne efterspørger kompetencer, der omfatter sikkerhed og compliance, hvilket falder ind under cybersikkerhed og risikohåndtering.

I rapporten Cybersikkerhed i små og mellemstore danske produktionsvirksomheder 2024[3] peger det samlede resultat på, at der er et stort udviklingsbehov inden for cybersikkerhed og supply chain risk management i produktionsvirksomhederne. Virksomhederne anerkender, at sikkerhedspraksisser er nødvendige for at kunne håndtere cybertrusler og risici, for at beskytte sig mod cyberangreb og dermed sikre forretningen digitalt.

I rapporten, Digital sikkerhed i danske SMV'er 2024, udført af Styrelsen for Samfundssikkerhed[3], fremhæves, at trusselsniveauet for cyberspionage og cyberkriminalitet er meget højt for danske virksomheder, og at der samtidig er stor efterspørgsel efter IT-specialister i både små, mellemstore og store virksomheder til at varetage virksomhedernes digitale sikkerhed.

Tendensen er, at mindre virksomheder enten benytter egne medarbejdere eller eksterne leverandører til at varetage den digitale sikkerhed, mens de store virksomheder både anvender egne medarbejdere og eksterne leverandører. Hvis virksomheden udelukkende benytter egne ansatte til at varetage it-sikkerhedsmæssige opgaver, bliver disse ofte delegeret til én af følgende tre medarbejderprofiler: 1) IT-specialister, 2) bogholdere eller 3) compliance- og kommunikationsspecialister. Ud over disse tre medarbejderprofiler bekræfter denne undersøgelse, at hele 77 pct. af SMV'erne udliciterer deres IT-sikkerhed til eksterne leverandører. Men selvom virksomheden udliciterer deres digitale sikkerhed, er det vigtigt, at virksomhederne har kompetencerne til at stille krav om, at der er styr på sikkerheden hos leverandøren, og dermed er det nødvendigt med et vist kompetenceniveau internt i virksomhederne.

Rapporten nuancerer de tre medarbejderprofiler, der hver især har deres tilgang til IT-sikkerhed. IT-specialisterne har ofte den fordel, at de kender de tekniske systemer i virksomheden, men i mindre grad det organisatoriske og forretningsmæssige perspektiv. Bogholderne har den fordel, at de arbejder tæt på ledelsen og kender til det organisatoriske perspektiv, men de mangler ofte de mere tekniske kompetencer.

Kommunikationsspecialisterne har den fordel, at de er dygtige til at lave kommunikationsværktøjer og strategier, men i mindre grad har indsigt i praksis i virksomhedens IT og produktion. Den samme udfordring gælder for eksterne IT-sikkerhedsleverandører.

Dette peger på, at der er forskellige behov for efteruddannelse for at understøtte de forskellige kompetencer, der er nødvendige for de forskellige medarbejderprofiler, som har ansvaret for digital sikkerhed i virksomheden. Dermed er der et behov for, at efteruddannelsestilbuddet imødekommer uddannelse af forskellige profiler med udgangspunkt i deres forskellige uddannelses- og erfaringsgrundlag.

Konklusion – aftagernes perspektiver på masteruddannelsen

Aftagerne udtrykker et aktuelt og stigende behov for at uddanne flere med kompetencer inden for cybersikkerhed og risikohåndtering, både regionalt og nationalt. De finder det relevant i alle typer af virksomheder og organisationer, uanset virksomhedens størrelse, og uanset om virksomheden supplerer med eksterne ydelser til at løfte opgaven med cybersikkerhed og risikohåndtering.
Enkelte aftagere har kommenteret, at læring om cybersikkerhed og risikohåndtering også kan tage form gennem andre uddannelsesmuligheder, eksempelvis som en kandidatuddannelse.

Størstedelen af aftagerne ser et behov og mener, at det er relevant at oprette en masteruddannelse inden for området, med fokus på at integrere både cybersikkerhed og risikohåndtering. De fremhæver, at hvis uddannelsen gøres mere fleksibel, eksempelvis med mulighed for at tage ét semester eller ét fag, så vil den være endnu mere interessant, realistisk og tidssvarende i forhold til den måde, virksomhederne opgraderer deres medarbejderes kompetencer på. Årsagen skal findes i begrænsede ressourcer, som gør, at nogle virksomheder i mindre grad benytter sig af længerevarende efteruddannelser. Desuden er rollerne inden for cybersikkerhed og risikohåndtering ofte fordelt på flere personer i virksomheden, der har forskellige arbejdsopgaver og fokus på den komplekse opgave med at sikre virksomheden digitalt.

Samtlige aftagere fremhæver, at der bør lægges særlig vægt på at tydeliggøre, hvilke profiler der kan søge ind, hvilke valgfag der kan vælges, og dermed også, hvilke konkrete kompetencer og hvilket udbytte man kan forvente efter endt uddannelse. I den forbindelse understreges det også, at der bør være ekstra fokus på målgruppen, og at denne ikke bør være for snæver, så ansøgere med atypiske profiler også har mulighed for at søge ind.

Aftagerne finder det faglige indhold og sammensætningen af uddannelsen ambitiøs og meget relevant. De har forskellige vægtninger af, hvilke fagelementer de vurderer som særlig betydningsfulde for deres virksomhed. De samlede og udtrykte betydningsfulde fagelementer er fremhævet nedenfor, og disse er allerede en del af uddannelsens indhold:

- Risikostyring med fokus på til- og fravalg samt en grundlæggende forståelse af trusler og IT-sikkerhed, herunder det forebyggende aspekt i arbejdet med risici.
- Evnen til at vurdere, omsætte og forbinde konkrete rammeværktøjer med ISO-standarder (NIS2, CIS, CIS18) til egen praksis i virksomheden.
- Et generelt fokus på læring og forståelse af kompleksiteten inden for cybersikkerhed og risikohåndtering, herunder infrastruktur og databeskyttelse.
- Rollen som kommunikatør i relation til risici, awareness og sikkerhed bredt i virksomheden samt på strategisk niveau.

Aftagerne fremhæver følgende kurser på uddannelsen, som særligt vigtige og interessante: computernetværk og cloud computing, principper for cybersikkerhed og resiliens i forsyningskæden, forbedret trusselmodellering og risikostyring, virksomhedens sikkerhedsarkitektur, anvendt cybersikkerhed og software operations. De fremhæver desuden, at det er en styrke, at den afsluttende masteropgave målrettes en problemstilling i egen virksomhed.

Af nye perspektiver anbefaler flere af aftagerne, at det vil tilføre mere værdi til uddannelsen, hvis der etableres et vedvarende fagligt netværk, som sikrer kontinuerlig læring samt løbende mulighed for at følge udviklingen inden for cybersikkerhed og risikohåndtering.

Af andre opmærksomheder i forbindelse med oprettelse af uddannelsen, anbefaler flere aftagere et øget fokus på formidlingen af uddannelsen, herunder forventninger til de praktiske og logiske forhold undervejs på uddannelsen, såsom hyppigheden af fremmøde, det forventede antal opgaver og den tid, der skal afsættes for at kunne følge uddannelsen. Derudover bør der lægges særlig vægt på formidlingen af gevinsten ved at gennemføre uddannelsen.

Anbefalinger og pointer fra SDU's aftagerundersøgelse

I det følgende fremhæves de vigtigste anbefalinger fra SDU's aftagerundersøgelse (2025) som hovedpointer, hvor ledere og nøglepersoner på tværs af brancher i det danske erhvervsliv har bidraget med perspektiver til udvikling af masteruddannelsen i cybersikkerhed og risikohåndtering på SDU i Odense:

- **Der er behov for efteruddannelse inden for cybersikkerhed og risikohåndtering**
- **Indfør mere fleksibilitet, og uddannelsen bliver endnu mere attraktiv for flere virksomheder**
- **Fokus på profilen: Skab klar sammenhæng mellem adgangskriterier, målgruppe, kurser og resultat**
- **Uddannelsens indhold og sammensætning er ambitiøs og relevant for virksomhederne**
- **Etablering af et vedvarende fagligt netværk**
- **Fokus på formidlingen af gevinsten ved at gennemføre uddannelsen samt på uddannelsens praktiske forhold**

Med ovenstående anbefalinger og pointer har SDU revideret uddannelsens indhold og har fået bekræftet nogle særlige fokuspunkter, der skal forankres i uddannelsen:

Revision af uddannelsens indhold efter aftagernes anbefalinger

- **Der er behov for efteruddannelse inden for cybersikkerhed og risikohåndtering**
  Forskningsmiljøet ser tilsvarende behov for efteruddannelsen inden for cybersikkerhed og risikohåndtering, som aftagerne. Forskningsmiljøet er desuden enige med aftagerne om at SDU skal fokusere på at imødekomme uddannelseskløften. Derfor er denne masteruddannelse målrettet et interdisciplinært fokus, fordi cybersikkerhed og risikohåndtering er et komplekst felt der spænder over både områderne IT og organisation, dette er allerede indarbejdet i uddannelsen og vil fremhæves yderligere. Uddannelsesfeltets nuværende tilbud har typisk et enten teknisk eller organisatorisk fokus, hvilket betyder, at denne uddannelse adskiller sig ved at integrere begge perspektiver i én.

- **Indfør mere fleksibilitet, og uddannelsen bliver endnu mere attraktiv for flere virksomheder**
  Forskningsmiljøet vil gerne understøtte aftagernes udtrykte behov ved at muliggøre, at man kan tage dele af masteruddannelsen, ét fag eller ét semester. Derved imødeses det, at rollen ofte vil være fordelt på flere nøglepersoner i en virksomhed. Desuden imødekommer det også, at virksomheder, uanset størrelse, ressourcer eller brug af konsulentydelser, får mulighed for gradvist at opgradere til det anbefalede vidensniveau inden for cybersikkerhed og risikohåndtering internt i virksomheden eller organisationen.

- **Fokus på profilen: Skab klar sammenhæng mellem adgangskriterier, målgruppe, kurser og resultat**
  Forskningsmiljøet vil gerne imødekomme aftagernes udtrykte behov ved at fremhæve yderligere retning og præcisering af profilerne i uddannelsen. Derfor har miljøet, med afsæt i feedback og det faglige aspekt, vurderet, at masteruddannelsen i cybersikkerhed og risikohåndtering kan uddanne to forskellige profiler, som fremhævet i følgende, og som er indarbejdet i uddannelsen og ansøgningen herom.

  Profil 1 har allerede stærke IT-kompetencer med en bachelor-, kandidat- eller tilsvarende diplomuddannelse fra en videregående uddannelsesinstitution. Til denne profil anbefaler forskningsmiljøet, at de studerende vælger valgfag inden for det organisatoriske spor på første semester. Målet er, at Profil 1 tidligt skal opbygge organisatoriske kompetencer med fokus på cybersikkerhed og risikostyring, og derefter gradvist udvikle et bredere kompetencesæt, der inkluderer både tekniske og organisatoriske perspektiver gennem hele uddannelsen.

  Ved afslutningen af uddannelsen vil denne profil kombinere avanceret IT- og sikkerhedsekspertise med solid organisatorisk indsigt. Dette vil gøre dem i stand til ikke blot at kommunikere mere effektivt med ledelsen om tekniske risici og behov, men også aktivt at bidrage til at tilpasse IT- og cybersikkerhedsstrategier med overordnede forretningsmål. Det positionerer dem til at påtage sig øgede strategiske og ledelsesmæssige ansvarsområder i deres virksomhed eller organisation.

  Profil 2 har allerede stærke kompetencer inden for områder uden for IT, med en baggrund tæt på organisation, ledelse og administration fra en bachelor-, kandidat- eller tilsvarende diplomuddannelse fra en videregående uddannelsesinstitution. Til denne profil anbefales det på første semester at vælge valgfag fra IT-sporet. Målet er, at Profil 2 tidligt i uddannelsen opbygger en solid forståelse af IT-systemer og cybersikkerhed og derefter gradvist udvikler en bredere færdighedsprofil inden for cybersikkerhed og risikostyring, der integrerer både IT- og organisatoriske kompetencer.

  Ved afslutningen af uddannelsen vil denne profil besidde stærke organisatoriske og kommunikationsevner, suppleret med en solid forståelse af IT-systemer, cybertrusler og afbødningstiltag. Dette vil gøre, at de bedre kan samarbejde med interne IT-afdelinger og eksterne sikkerhedsudbydere samt kunne integrere digital risikostyring i strategisk forretningsplanlægning og drift.

  For at imødese aftagernes feedback om øget fleksibilitet i måden at tage uddannelsen på imødekommer fagmiljøet, at begge profiler også kan vælge fag frit samt tage enkelte fag og semestre isoleret eller løbende, afhængigt af behov, muligheder og erfaringsgrundlag.

- **Uddannelsens indhold og sammensætning er ambitiøs og relevant for virksomhederne**
  Fagmiljøet har vurderet, at de fremhævede og ønskede kompetencer allerede er en del af indholdet på uddannelsen. Valgfagene samt fleksibiliteten i måden, uddannelsen kan tages på, gør det muligt for ansøgerne at tilpasse og vægte deres profil i en specifik og ønsket retning. Miljøet vil sørge for, at de fremhævede fokus- og fagelementer fra aftagerne, indføres tydeligere som en del af beskrivelserne på uddannelsens kurser samt efterfølgende i undervisningen på uddannelsen.

- **Etablering af et vedvarende fagligt netværk**
  Forskningsmiljøet vil gerne understøtte aftagernes anbefaling om etablering af et fagligt netværk og arbejder på at oprette et hub inden for området, hvor forskere og virksomheder kan mødes om cybersikkerhed og risikohåndtering. Foreløbigt er det drøftet, at mødes om cybersikkerhed og risikohåndtering i relation til nye risici, trends, standarder, metoder, værktøjer og teknologier, for eksempel med introduktion af software, der hjælper med at analysere sårbarheder i forsyningskæder. Udviklingen af dette hub er i gang internt på Institut for Matematik og Datalogi ved det Naturvidenskabelige Fakultet, med overvejelser om at øge det tværfaglige aspekt ved eventuelt at inddrage relevante forskningsmiljøer fra det Samfundsvidenskabelige Fakultet på SDU.

- **Fokus på formidlingen af gevinsten ved at gennemføre uddannelsen samt på uddannelsens praktiske forhold**
  Forskningsmiljøet og ledelsen er opmærksomme på at afsætte ressourcer til markedsføringsindsatsen, der er målrettet gevinsten ved at gennemføre uddannelsen, samt til formidlingen af uddannelsens praktiske forhold.

Med ovenstående justeringer imødekommer SDU's masteruddannelse i cybersikkerhed og risikohåndtering arbejdsmarkedets og aftagernes behov i forhold til behov, indhold, muligheder og kompetencer.

Metode

Evidens

National strategi for cyber- og informationssikkerhed 2022-2024[1].
I det følgende præsenteres de store linjer fra Danmarks nationale gældende strategi for cyber- og informationssikkerhed:

Danmark er en af verdens førende nationer, når det gælder digitalisering. Digitalisering er en afgørende drivkraft for udviklingen af det danske samfund. Men med den høje grad af digitalisering følger også en øget sårbarhed over for kriminelle, der forsøger at udnytte sårbarhederne i vores digitale samfund. Regeringen anser cybertruslen for en af de mest alvorlige trusler mod Danmark. Hver dag er myndigheder, virksomheder og borgere mål for cyberangreb i større eller mindre skala. Hackere, kriminelle og fjendtlige efterretningstjenester sætter danskernes digitale sikkerhed under pres. Den digitale udvikling går stærkt, og nye cyberangrebsformer kommer til i samme hast. Derfor er der behov for en styrket indsats, hvis vi skal følge med og være på forkant med udviklingen i trusler og digitale sårbarheder.

Den danske strategi har fokus på både stat, kritisk infrastruktur, borgerne og erhvervslivet. Den udefrakommende cybertrussel, kræver en fælles indsats, hvis vi skal beskytte Danmark mod cyberkriminalitet og cyberspionage. Regeringen har allerede styrket cyberreserven, og nu styrkes indsatsen yderligere med den nationale strategi for cyber- og informationssikkerhed. Med strategien udmønter regeringen i alt 270 mio. kr. til 34 nye hovedinitiativer, som bidrager til, at vi i Danmark kan færdes sikkert digitalt.

Truslen fra cyberkriminalitet og cyberspionage er i dag meget høj, og det samme forventes i fremtiden. Den digitale infrastruktur er i stigende grad en forudsætning for, at vores samfund fungerer. Men jo flere digitale systemer, vi anvender og kobler sammen, desto flere steder kan vi blive udsat for angreb. Samtidig er spionagetruslen fra fremmede staters efterretningsvirksomhed blevet mere markant. Fremmede staters efterretningstjenester anvender teknologiske fremskridt og gør brug af avancerede hackergrupper, der gennem cyberangreb er i stand til at få adgang til it-systemer for at udøve efterretningsvirksomhed mod Danmark. Angrebene er ofte komplekse, og såvel politikere, embedsfolk og myndigheder som forskningsinstitutioner og virksomheder kan indgå som enten mål eller middel i disse aktiviteter. Samtidig står en række nye digitale muligheder, såsom kunstig intelligens, big data, kvanteteknologi og 5G, for døren. Dette stiller høje krav til, hvordan vi som samfund håndterer vores beskyttelsesværdige informationer og den digitale infrastruktur, som er afgørende for opretholdelsen af vores samfundsvigtige funktioner. Ligeledes stiller det krav til de virksomheder, der indgår i forsyningskæderne.

Fra EU er der også et stort fokus på at højne cybersikkerheden med nedenstående direktiv om sikkerhed i net- og informationssystemer i samfundskritiske sektorer. Det stiller også krav til, at Danmark øger ambitionsniveauet, herunder hvad angår risikostyret ledelsesforankring, implementering af sikkerhedsforanstaltninger og IT-beredskab:

Direktiv om sikkerhed i net- og informationssystemer i samfundskritiske sektorer (NIS-direktivet)

EU-direktivet om sikkerhed i net- og informationssystemer i samfundskritiske sektorer (NIS-direktivet) fra 2016 er et væsentligt instrument i at højne cyber- og informationssikkerheden i de samfundsvigtige sektorer i Danmark. I december 220 fremsatte Kommissionen et forslag til revision af direktivet, hvor der lægges op til at udvide direktivets dækningsområde i bredden og dybden

bl.a. i form af nye krav til cybersikkerheden i de omfattende virksomheder og myndigheder samt til medlemsstaternes tilsyn med cybersikkerheden. Formålet er ledelsesforankret risikostyring, implementering af organisatoriske og tekniske foranstaltninger samt styr på beredskabet, der gør organisationer i stand til hændelseshåndtering (før, under og efter) og operativt samarbejde på tværs af organisationer og landegrænser i EU.

I strategien fremhæves det også, at fokus på erhvervslivets cyber- og informationssikkerhed skal være en prioritet for alle danske virksomheder, herunder særligt de små og mellemstore virksomheder (SMV'er), fordi mange af de ca. 300.000 danske SMV'er rammes af cyberangreb, og tendensen er stigende. Et cyberangreb kan i yderste konsekvens betyde, at en virksomhed mister sit forretningsgrundlag.

Strategien har fire målsætninger, der danner rammen for udviklingen mod et stærkere og mere sikkert digitalt Danmark. Særligt de to første målsætninger taler ind i, at nye krav giver nye opgaver, og det kalder på, at relevante nøglepersoner i virksomheder og organisationer opkvalificeres med nye kompetencer inden for cyber- og informationssikkerhed, for at kunne sikre det nødvendige sikkerhedsniveau:

Fra første målsætning: **"***Statslige myndigheder og virksomheder skal have et tilfredsstillende sikkerhedsniveau og skal med kort varsel være i stand til at agere i tilfælde af alvorlige cyberhændelser."*

Fra anden målsætning: *"Cyber- og informationssikkerhed skal være forankret i topledelsen, og kompetencerne skal styrkes. Det gælder ift. overblik over aktiver, sårbarheder og kendskab til potentielle trusler. Borgere, virksomheder og statslige myndigheder skal vide, hvordan de beskytter sig og færdes sikkert digitalt. Efterspørgslen på cyber- og informationssikkerhedskompetencer skal imødekommes ved at uddanne flere specialister og opbygge stærkere kapacitet på tværs af samfundet."*

Med området følger en række centrale udfordringer, herunder manglende forståelse for cybertruslen samt komplekse IT-systemer. I dag har 40 pct. af de danske små og mellemstore virksomheder et digitalt sikkerhedsniveau, der er utilstrækkeligt i forhold til deres risikoprofil, og mange virksomheder mangler helt grundlæggende tiltag i deres digitale sikkerhed. Der er derfor behov for at styrke den digitale robusthed i de danske virksomheder. Til dette ligger der en tværgående udfordring i både at rekruttere såvel som at fastholde relevante kompetencer inden for cyber- og informationssikkerhedsområdet: *"For efterspørgslen på cyber- og informationssikkerhedskompetencer er stor, både myndigheder og virksomheder oplever, at det er vanskeligt at skaffe de rette profiler til opgaverne. Der er derfor behov for at styrke udbuddet af kompetencer, hvis sikkerheden skal løftes bredt set."*

Strategien fremhæver en mangel på kompetencer og et behov for mere uddannelse inden for området cybersikkerhed og risikohåndtering i Danmark.

IT-branchens årlige brancheanalyse fra 2024[(2)] viser, at manglen på it-kompetencer er den absolut største barrierer for vækst i it-branchen. 40% af virksomhederne efterspørger kompetencer, der omfatter sikkerhed og compliance, hvilket falder under cybersikkerhed og risikohåndtering. Undersøgelsen er blevet gennemført siden 2013, og i 2024 deltog 201 it-virksomheder via et onlinespørgeskema.

Rapporten, Cybersikkerhed i små og mellemstore danske produktionsvirksomheder 2024[(3)], er et delresultat i projektet "Cybersikkerhed og Forretningskontinuitet". Rapporten er en del af et forskningsprojekt, der er gennemført af forskere fra Institut for Erhverv og Bæredygtighed, SDU, Center for War Studies, SDU, Institut for Matematik og Datalogi, SDU, samt Forsvarsakademiet. Den tager afsæt i en landsdækkende spørgeskemaundersøgelse, der har fokus på danske små og mellemstore produktionsvirksomheders praksis med cybersikkerhed. I alt har 248 virksomheder deltaget i undersøgelsen.

Danske virksomheder handler og samarbejder i stort omfang med kunder og leverandører i Danmark såvel som globalt. Samhandlen og den tiltagende digitalisering betyder, at virksomhederne i dag er meget tæt integreret, også i cyberspace. Det er en god ting, og det gør det muligt for virksomhederne at skabe

konkurrencedygtige forretningsmodeller og levere markedsledende produkter af høj kvalitet. Men de tætte bånd i værdikæderne betyder, at danske virksomheder skal være ekstra opmærksomme. En kæde er aldrig stærkere end det svageste led, og svigter sikkerheden hos en leverandør, så smitter det hurtigt. Derfor er koblingen af cybersikkerhed og værdikæder afgørende.

I rapportens resultater fremhæves det, at produktionsvirksomhederne har en stor grad af opmærksomhed på cybersikkerhed og anerkender, at sikkerhedspraksisser er nødvendige for at kunne håndtere cybertrusler- og risici for at beskytte sig mod cyberangreb. Det samlede resultat peger på et stort udviklingsbehov inden for cybersikkerhed og supply chain risk management i virksomhederne.

I rapporten, Digital Sikkerhed i Danske SMV'er 2024[3], udført af Styrelsen for Samfundssikkerhed fremhæves det også her, at trusselsniveauet for cyberspionage og cyberkriminalitet er meget højt for danske virksomheder. Alligevel har mange virksomheder, særligt små og mellemstore virksomheder (SMV'er), ikke tilstrækkeligt fokus på digital sikkerhed. Det skyldes blandt andet, at mange af dem ikke ser sig selv som interessante mål for hackerne, og derfor ikke prioriterer de nødvendige ressourcer til at sikre sig. For det kræver både ressourcer i form af tid og penge samt de rette kompetencer at arbejde helhedsorienteret med cybersikkerhed.

Datagrundlaget i rapporten er beregnet på baggrund af Danmarks Statistiks årlige spørgeskemaundersøgelse "IT-anvendelse i virksomheder". Rapporten baserer sig på data indsamlet i 2023, der består af besvarelser fra 4.557 virksomheder inden for de private, ikke-finansielle erhverv. Det er obligatorisk for virksomheder at besvare undersøgelsen. Desuden er data vægtet, så resultaterne afspejler populationen af danske virksomheder. Rapporten "Digital sikkerhed i danske SMV'er" er gennemført årligt siden 2020.

I rapporten fremhæves det, at der fortsat er et markant behov for at løfte den digitale sikkerhed blandt de danske SMV'er, da hele 40 pct. af SMV'erne fortsat ikke har et digitalt sikkerhedsniveau, som matcher deres risikoprofil. SMV'erne er sårbare over for angreb, der vil lamme deres systemer, da 60 pct. af dem slet ikke eller kun i lav grad vil kunne udføre virksomhedens kerneopgaver uden adgang til interne centrale it-systemer.

Et cyberangreb kan være meget omkostningstungt for en virksomhed, og det kan have store konsekvenser. Virksomhedens ledelse bærer derfor ansvaret for virksomhedens digitale sikkerhed. Men besvarelserne i denne analyse viser, at under halvdelen (40 pct.) af ledelserne i de danske SMV'er i høj grad tager stilling til virksomhedernes it-sikkerhedsmæssige aktiviteter, mens 17 pct. slet ikke eller kun i lav grad tager stilling. Rapporten fremhæver, at jo højere grad ledelsen tager stilling til virksomhedens it-sikkerhedsmæssige aktiviteter, des højere er virksomhedens it-sikkerhedsniveau.
En anden forklaring på, at SMV'erne ikke er i mål med den digitale sikkerhed er, at 37 pct. af SMV'erne oplever udfordringer eller begrænsninger med at øge virksomhedens digitale sikkerhedsniveau, fordi de blandt andet mangler kompetencer til at håndtere it-sikkerhedsløsninger, eller har begrænsede ressourcer til at investere i deres it-sikkerhed.

Tendensen er, at mindre virksomheder enten benytter egne medarbejdere eller eksterne leverandører til at varetage den digitale sikkerhed, mens de store virksomheder både anvender egne medarbejdere og eksterne leverandører. Anvender virksomheden udelukkende egne ansatte til at varetage it-sikkerhedsmæssige opgaver, er det særligt vigtigt, at disse medarbejdere har de rette kompetencer.
I rapporten indikeres det, at der i både små, mellemstore og store virksomheder er stor efterspørgsel efter IT-specialister, og udbuddet overgår efterspørgslen. Desuden har SMV'erne typisk ikke en decideret it-sikkerhedsekspert ansat, men ansvaret for it-sikkerhed bliver ofte delegeret til én af følgende tre medarbejderprofiler: 1) IT-specialister, 2) bogholdere eller 3) compliance- og kommunikationsspecialister. Ud over de tre medarbejderprofiler bekræfter undersøgelsen, at mange SMV'er udliciterer deres it-sikkerhed til eksterne leverandører. Samlet set benytter hele 77 pct. af SMV'erne sig (i et vist omfang eller helt) af ekstern hjælp til at løfte virksomhedens digitale sikkerhed.

Der kan være mange fordele for en virksomhed i at udlicitere dens it-sikkerhedsmæssige aktiviteter til eksterne leverandører. For eksempel har mange af de mindre SMV'er hverken behov for eller ressourcer til at

ansætte en decideret it-sikkerhedsekspert eller en it-afdeling. Men selvom virksomheden udliciterer deres digitale sikkerhed, er det fortsat vigtigt, at virksomhederne har kompetencerne til at stille krav til, at der er styr på sikkerheden hos leverandøren. Her viser resultaterne, at der er plads til forbedring, da 25 pct. af de SMV'er, som anvender en ekstern leverandør, ikke stiller krav til leverandøren om for eksempel behandling af data, it-sikkerhedsforanstaltninger og/eller løbende dokumentation om it-sikkerhed. Til trods for, at mange virksomheder udliciterer ansvaret for deres it-sikkerhed, indikerer rapporten også, at det er nødvendigt med et vist kompetenceniveau internt i virksomhederne.

Undersøgelsen nuancerer de tre medarbejderprofiler, der har hver deres tilgang til it-sikkerhed, herunder forskellige styrker og svagheder i forhold til at varetage opgaven. IT-specialisterne har ofte den fordel, at de kender de tekniske systemer i virksomheden, men i mindre grad det organisatoriske og forretningsmæssige perspektiv. Bogholderne har den fordel, at de arbejder tæt på ledelsen og kender til det organisatoriske perspektiv, men de mangler ofte de mere tekniske kompetencer. Kommunikationsspecialisterne har den fordel, at de er dygtige til at lave kommunikationsværktøjer og strategier, men i mindre grad har indsigt i praksis i virksomhedens IT og produktion. Den samme udfordring gælder for eksterne IT-sikkerhedsleverandører.

Der er således på forskellig vis "huller" eller behov for efteruddannelse i forhold til at understøtte SMV'ernes digitale sikkerhed, afhængigt af hvilke medarbejderprofiler, der har ansvaret for opgaven. Dette kalder på et behov for at efteruddannelses-udbuddet imødeser at uddanne forskellige profiler med afsæt i forskellige medarbejderbaggrunde, så alle profiler, nøglepersoner inden for cybersikkerhed og risikohåndtering, vil kunne opnå tilstrækkelig læring og dermed integrere cybersikkerhed og risikohåndtering og sikre virksomhederne digitalt.

Aftager

I 2025 har SDU gennemført en bred aftagerundersøgelse på tværs af brancher, hvor ledere og nøglepersoner inden for cybersikkerhed har bidraget med deres perspektiver på, om der er et regionalt og nationalt behov for en masteruddannelse inden for cybersikkerhed og risikohåndtering, uddannet på Syddansk Universitet i Odense.

I aftagerundersøgelsen indgår virksomheder og organisationer fra både den private og offentlige sektor. Virksomhederne varierer i størrelse fra mindre og mellemstore til store. Der er givet støtteerklæringer til uddannelsen fra fire virksomheder, et erhvervshus og en interesseorganisation.

I det følgende belyses de første aftagers perspektiver på uddannelsesidéen:

Cybersikkerhed og Forretningskontinuitet, januar 2025.

Uddannelsesidéen blev præsenteret på et styregruppemøde i Cybersikkerhed og Forretningskontinuitet i januar 2025. På mødet deltog repræsentanter fra: Dansk Industri (DI), DI2X – Digital Leadership Research Institute, KFISCH, Zoriac Aps. Fra SDU, Dekanen på Det Naturvidenskabeligt Fakultet samt repræsentanter for Institut for Matematik og Datalogi, Center for War Studies, Institut for Erhverv og Bæredygtighed og Forsvarsakademiet.

Repræsentanterne var overordnet positive omkring oprettelsen af masteruddannelsen i cybersikkerhed og risikohåndtering og bekræftede, at der er et behov for at uddanne flere specialister med kompetencer inden for cybersikkerhed og risikohåndtering i Danmark.

Repræsentanterne fremhævede uddannelsens fokus på risikoforebyggelse som særligt positivt, da dette er et nyt fokus, som ingen andre uddannelser i Danmark imødeser.

Repræsentanterne var særligt opmærksomme på det kommunikative aspekt, herunder at genoverveje titlerne på kurserne, så de er mere retvisende for indholdet. Det blev fremhævet, at informationen om profilen for uddannelsen bør målrettes, herunder med fokus på, hvad virksomhedsledere får ud af at sende en medarbejder på denne master, samt hvilke kompetencer man konkret får med i værktøjskassen. Der blev også gjort opmærksom på at sikre og fremhæve den akademiske progression i uddannelsens sammensætning.

Udover at være i dialog med styregruppen har SDU foretaget i alt 16 interviews med nøglepersoner fra nedenstående virksomheder. Virksomhederne er både forankret i og uden for Region Syddanmark og varierende i størrelse:

Interview med 16 virksomheder:

- Fire Eater (mindre virksomhed)
- Terma (stor virksomhed)
- KFISCH, DIIS, Dansk Institut for Internationale Studier samt Forsvarsministeriet (mindre og mellemstor virksomhed).
- Dansk Gummi Industri (mindre virksomhed)
- Gomspace (mellemstor virksomhed)
- Rambøll (stor virksomhed)
- Sparrow Quantum (mindre virksomhed)
- Digital Frontier (mindre virksomhed)
- Orifarm (mellemstor virksomhed)
- Odense Kommune (stor organisation)
- Jeros (mindre virksomhed)
- Dansk Sintermetal (mindre virksomhed)
- HMK Bilcon (mellemstor virksomhed)
- Unik Systemdesign (mellemstor virksomhed)
- Energinet (stor virksomhed)
- Bankdata (stor virksomhed)

Der er i alt givet seks støtteerklæringer til oprettelse af masteruddannelsen i cybersikkerhed og risikokohåndtering:

Støtteerklæringer fra følgende aftagere:

- KFISCH
- Dansk Gummi Industri
- Rambøll
- Unik Systemdesign

Støtteerklæringer fra interesseorganisation og erhvervshus (som ikke har deltaget i et interview):

- Technology Denmark
- Erhvervshus Fyn

Interviewene er dialogbaserede og udført med en semistruktureret tilgang, hvor aftagerne forinden præsenteres for en interview- og informationsguide udsendt via mail. Denne indeholder informationer om uddannelsens ramme herunder, optagelseskriterier, formål og profilen dimittenderne opnår på uddannelsen samt indholdet på uddannelsens kurser.

Nedenstående spørgsmål danner ramme for interviewet:

- I hvor høj grad ser du/I et behov for at efter- og videreuddanne medarbejdere inden for cybersikkerhed og risikohåndtering i form af en 2-årig (deltids) masteruddannelse?

- Vil I overveje at tilbyde denne masteruddannelse til én eller flere ansatte i jeres virksomhed?
- Ud fra dit kendskab til virksomhedens opgaver inden for cybersikkerhed og risikohåndtering, i hvor høj grad passer nedenstående kompetencer/kurser til opgaveløsningen i jeres virksomhed?
- Har du/I forslag til, hvilke kompetencer der bør styrkes, eller som I anser for at være særligt vigtige at prioritere på uddannelsens kurser, så det bliver attraktivt at sende jeres medarbejdere på denne masteruddannelse?
- Har du/I forslag til nye kompetencer, som I eventuelt finder manglende i uddannelsesudkastet, så det bliver endnu mere attraktivt at sende jeres medarbejdere på denne masteruddannelse?
- Er der andre aspekter, vi skal være opmærksomme på i forbindelse med oprettelsen af denne masteruddannelse?

Støtteerklæringer

Efter interviewene er udvalgte aftagere blevet spurgt, om de vil give en støtteerklæring til oprettelsen af SDU's masteruddannelse i cybersikkerhed og risikohåndtering. De samlede støtteerklæringer findes på side 26.

Resultater

Dette afsnit af aftagerrapporten er baseret på i alt 16 forskellige interviews med nøglepersoner fra forskellige virksomheder.

Som tidligere nævnt er interviewene dialogbaserede, og derfor går de forskellige interviews i mindre grad i forskellige retninger i forhold til, hvad der er relevant for den enkelte virksomhed eller organisation. Derfor er det heller ikke alle spørgsmål, der indgår i dialogen. Svarene med disse nuancer er afspejlet i de udvalgte udtalelser fra aftagerne.

Resultaterne fra aftageundersøgelsen er tematiseret i 2 områder; 1) behovet for masteruddannede dimittender inden for cybersikkerhed og risikohåndtering nationalt og regionalt, 2) uddannelsens indhold og sammensætning.

1. Behovet for masteruddannelse inden for cybersikkerhed og risikohåndtering

Nedenstående viser en oversigt over, i hvor høj grad aftagerne har udtrykt, at virksomheden eller organisationen ser et behov for masteruddannede dimittender med kompetencer inden for cybersikkerhed og risikohåndtering:

Aftagere	I høj grad	I mindre grad	Slet ikke
Fire Eater	X		
Terma	X		
KFISCH, DIIS og forsvarsministeriet	X		
Dansk Gummi Industri	X		
Gomspace	X		

Rambøll	X		
Sparrow Quantum	X		
Digital Frontier	X		
Orifarm		X	
Odense Kommune	X		
Jeros	X		
Dansk Sintermetal		X	
HMK Bilcon	X		
Unik Systemdesign	X		
Energinet		X	
Bankdata	X		

Nedenstående udtalelser viser nuancerne i aftagernes behov for masteruddannede dimittender inden for cybersikkerhed og risikohåndtering, samt nuancerne i virksomheden eller organisationens villighed og overvejelser om at sende en medarbejder på en master i cybersikkerhed og risikohåndtering:

Uddannelsen er en god idé, dog er to år lang tid at undvære en medarbejder delvist. Vi har i det seneste år arbejdet aktivt med tiltag, der skal forbedre cybersikkerheden i vores virksomhed, blandt andet med brug af afgrænsede konsulentydelser.
Vi har én mand, vi kan sende af sted på uddannelsen. Det vil umiddelbart være meget at sende ham afsted, og samtidigt vil jeg ikke være afvisende, fordi det ville være godt at have kompetencerne internt. Derfor vil jeg gerne høre om det, hvis uddannelsen bliver igangsat.
Det er meget vigtigt at præcisere tydeligt, hvilke profiler der kan søge ind i forbindelse med, hvilke valgfag man kan tage, og dermed også, hvilke konkrete kompetencer man ender ud med. Udbyttet af, hvad vi får ud af at sende en medarbejder afsted på uddannelsen, vil være afgørende - Fire Eater

Det er en god idé med en masteruddannelse, der bakker op om dette område. Der vil være et stigende behov for flere kompetencer inden for feltet, men I skal være opmærksomme på, hvilken målgruppe I tiltrækker, så den ikke er for snæver. Hvad er det konkrete udbytte, og hvilke mangler ser I, der er uddannelsesmæssigt, sammenlignet med øvrige uddannelsestilbud i Danmark.
Der er brug for fleksibilitet i denne type uddannelse. Kan uddannelsen for eksempel tages på fire år, og kan man vælge at tage kun ét semester uden at gennemføre hele uddannelsen. Disse muligheder skal kommunikeres tydeligt - Terma

Det handler om virksomhedernes sikkerhed. Masteruddannelsen er en rigtig god idé og et godt initiativ. Den kan sikre fremtidens virksomheder digitalt. I alle virksomheder og organisationer findes der nøglepersoner, også inden for dette felt, og det er disse personer, virksomhederne skal sende afsted på denne uddannelse - KFISCH, DIIS og forsvarsministeriet

Uddannelsen er et supergodt og vigtigt initiativ. Vi har dog outsourcet vores IT til en privat udbyder, da vi er en lille virksomhed. Men derfor skal der stadig være opmærksomhed internt, da de interne sikkerhedsrisici er nogle af de største. Vi forholder os åbent over for uddannelsesmuligheden, og det er positivt, at målgruppen er nøglepersoner inden for feltet og ikke ledere - Dansk Gummi Industri

Dette er superrelevant for IT-folk. De folk, vi har ansat, som det er relevant for, har ikke en kandidatgrad. For os er det mest interessant at sende en medarbejder afsted på ét semester ad gangen eller mindre,

fordi det vil være relevant for fire forskellige medarbejdere. Derfor vil adgangskriterier og muligheder for at tage enkelte dele af uddannelsen være afgørende for, om vi vil investere i det. Overvej, hvem jeres målgruppe er. For ti år siden var det mere almindeligt at sende medarbejdere afsted på disse typer uddannelser. Nu er det mere trenden at tage kortere kurser eller for eksempel, ét enkelt semester - Gomspace

Masteruddannelsen er en god idé, og den kommer på et godt tidspunkt, med stigende krav inden for området. Jeg kunne godt se, at uddannelsen vil være relevant for nøglemedarbejdere fra vores IT-organisation - Rambøll

Dette er meget relevant, både i forhold til den geopolitiske situation, og det er relevant, at masteruddannelsen kombinerer cybersikkerhed med risikohåndtering. En anden opmærksomhed er, at denne masteruddannelse også kan være interessant for NGO-organisationer, de har de samme udfordringer som alle andre, selvom den er særligt relevant for SMV'erne. Jeg ser kun, at behovet for denne rolle vil vokse i fremtiden i takt med den digitale udvikling. Vi er en lille virksomhed, men jeg kan godt forestille mig, at denne uddannelse vil være relevant for en medarbejder, der er ansvarlig for dette område - Sparrow Quantum

Uddannelsen er virkelig interessant, fordi den kombinerer det tekniske med det organisatoriske perspektiv. En udfordring inden for feltet er, at uddannelsesudbuddet er for teknisk tungt, men der er også behov for, at man kan arbejde med cyber- og risikoaspekter inden for begge perspektiver. Det er særligt i SMV'erne. Uddannelsen er sådan set relevant for mig, derudover ser jeg, at den er særlig relevant for SMV'erne. Men I skal overveje at åbne yderligere op for, hvem der kan søge ind på uddannelsen, da I risikerer at begrænse jer i forbindelse med optaget. Det er vigtigt, at jeres profil adskiller sig tydeligt fra de andre lignende uddannelsesprofiler - Digital Frontier

Der er et øget og stigende fokus på dette felt, og et stort behov for at uddanne medarbejdere med kompetencer inden for området. Spørgsmålet er, om en masteruddannelse er den bedste måde. Vi vil foretrække en kandidatuddannet inden for dette område, en specialist – hellere det end at sende en medarbejder på en lang efteruddannelse. Ellers kunne det være interessant, hvis der var mulighed for at kunne tage ét enkelt fag. Vi har seks til syv personer, der arbejder fuldtid med området, vi kan ikke drive vores forretning uden at have meget fokus på dette - Orifarm

Det er meget relevant at efteruddanne inden for området. I vores organisation er det almindeligt, at man tager længere uddannelsesforløb, som denne uddannelse. Jeg kan godt se relevansen af denne uddannelse - Odense Kommune

Det er en rigtig god idé. Hos os vil det være mig, der kan komme afsted på uddannelsen, og jeg synes, det ser rigtig spændende ud. Jeg kan blive i tvivl om, hvor jeres marked er, og hvor mange der vil prioritere og få mulighed for at tage på uddannelse i to år, selvom det er vigtigt. Vi tilkøber også konsulentydelser til at løse disse opgaver - Jeros

Vi er blevet mere bevidste om, at området er meget vigtigt. Vi er så små, at vi i stedet tilkøber hjælp til at løse opgaven udefra. Da vi er en lille virksomhed, og ikke er omfattet af NIS2, vil det for nuværende være mere relevant med et kort kursus eller tilkøb af ydelser, som vi allerede benytter os af - Dansk Sintermetal

Det er i høj grad relevant at efteruddanne inden for området, og indholdet er meget spot on. Jeg kan dog ikke se, at det er realistisk at kunne undvære mig på deltid i to år, og jeg er den eneste, der umiddelbart er relevant at sende afsted. Det er nok mere realistisk, hvis jeg kunne tage et eller flere af fagene. Vi har outsourcet en del af dette område til en privat udbyder, men hvis vi skulle ansætte én, der også skulle arbejde

med dette felt, ville det være interessant at finde en, der allerede var uddannet, og det ville ikke gøre noget, at det var en nyuddannet, erfaringen skal man nok få. I skal være obs på adgangskriterierne, I kan risikere at udelukke potentielle nøglepersoner med andre atypiske baggrunde - HMK Bilcon

Uddannelsen er et bedre alternativ end for eksempel en certificering. Vi er dog flere, der arbejder med dele af det, og en hel del af opgaverne er outsourcet, så det vil være en stor investering for en lille virksomhed. For nuværende kommer vi ikke til at sende en medarbejder afsted, selvom jeg kan se relevansen i at opgradere flere interne inden for feltet. Fleksibilitet i måden at tage uddannelsen på er vigtig, eksempelvis ved at muliggøre at tage dele af uddannelsen afhængigt af baggrund og erfaring. Det er en fordel at nudge de forskellige profilretninger - Unik Systemdesign

Vi har brug for specialiserede profiler, der har en mere teknisk cybersikkerhedsprofil. Jeres oplæg er meget bredt med brede optagelseskriterier. Det er vigtigt at kunne opnå tilstrækkelig læring og forståelse i de enkelte fag, for at kunne omsætte det til brug i virksomheden. De profiler, der er svære at finde, er dem med IT-teknisk baggrund, som også har opnået en teknisk funderet og specialiseret viden i cybersikkerhed. Et adgangskrav skal være, at man har en IT-baggrund, for at blive i stand til at opnå omsættelig og brugbar viden. Vi opgraderer kun medarbejdere med afgrænsede kompetencer i form af kortere kurser. Vi ville ikke sende en medarbejder afsted på en 2-årig uddannelse, da det vil være alt for lang tid at undvære ressourcen.
Der skal være en tydelig sammenhæng mellem, hvem målgruppen er, og hvilket konkret udbytte man får. Det er også vigtigt, at I tænker fleksibiliteten ind, hvis I går med en masteruddannelse, så man fx kun kan tage ét fag, fordi det kan være enkelte supplerende kompetencer, man mangler som medarbejder i en virksomhed. I de gængse IT-uddannelser er der meget lidt cybersikkerhed, og måske kunne cybersikkerhed tænkes ind som kandidatoverbygninger på en IT-bachelor - Energinet

Det er kun godt, at der kommer mere efteruddannelse inden for cybersikkerhed og risikohåndtering. Der dukker lige nu flere uddannelsesinitiativer og kurser op inden for området, så I skal være obs på at finde netop der, hvor uddannelsesbehovet eller manglen er. Vi ansætter typisk nyuddannede, der har haft et valgfag eller en særlig interesse i dette, og så oplærer vi dem. Ellers ansætter vi en allerede erfaren inden for området, så derfor vil jeg ikke umiddelbart sende en medarbejder af sted, medmindre jeg har en medarbejder, der skal omplaceres fra en afdeling til en anden.
Vi vælger også typisk kortere kurser og sidemandsoplæring. Hvis man kan tage enkelte fag eller semestre, vil det være mere interessant for os at sende en medarbejder af sted. Vær meget obs på jeres profilretninger, og gør det helt tydeligt for os – også gerne visuelt – hvad jeg får, hvis jeg vælger denne retning. Det hænger sammen med adgangskriterier, målgruppe og profilretning - Bankdata

Delkonklusion om behovet for en master i cybersikkerhed og risikohåndtering på SDU

- **Der er behov for efteruddannelse inden for cybersikkerhed og risikohåndtering**
  Aftagerne udtrykker et bredt, aktuelt og stigende behov for at uddanne flere med kompetencer inden for cybersikkerhed og risikohåndtering, og størstedelen finder denne masteruddannelse relevant. Flere understreger desuden, at vi skal være opmærksomme på at tilbyde uddannelse, hvor manglerne er. Dette er især vigtigt i forhold til andre lignende uddannelser inden for området, og fordi flere nye efteruddannelser inden for cybersikkerhed er under udvikling på tværs af Danmark. Enkelte aftagere har bidraget med perspektiver på, hvordan læring om cybersikkerhed og risikohåndtering også kan tage form gennem andre uddannelsesmuligheder f.eks. som en kandidatuddannelse.

- **Indfør mere fleksibilitet, og uddannelsen bliver endnu mere attraktiv for flere virksomheder**
  Aftagerne fremhæver, at hvis uddannelsen bliver mere fleksibel, for eksempel med mulighed for at sende medarbejdere af sted på ét semester eller ét fag, så vil det være endnu mere interessant, realistisk og tidssvarende i måden, virksomhederne opgraderer deres medarbejderes kompetencer på. Dette skyldes blandt andet manglende ressourcer, som gør, at virksomhederne i mindre grad benytter sig af længerevarende efteruddannelser, da det er for omkostningstungt at undvære ressourcerne. Desuden er rollerne inden for cybersikkerhed og risikohåndtering ofte fordelt på flere personer i virksomheden, og især i mindre virksomheder tilkøbes der ofte konsulentydelser fra eksterne udbydere. Samtidig ser virksomhederne også et stigende behov for at styrke kompetencerne inden for feltet internt i virksomheden uagtet tilkøb af ekstern hjælp.

- **Fokus på profilen: Skab klar sammenhæng mellem adgangskriterier, målgruppe, kurser og resultat**
  Samtlige aftagere fremhæver, at der bør lægges et særligt fokus på at fremhæve, hvilke profiler der kan søge ind i sammenhæng med, hvilke valgfag man kan tage, og dermed også, hvilke konkrete kompetencer og udbytte man ender med at opnå efter endt uddannelse. I denne sammenhæng fremhæves det ligeså, at der bør være ekstra fokus på målgruppen, og at den ikke er for snæver, for ansøgere med atypiske profiler.

2. Uddannelsens indhold og sammensætning

Aftagerne har forholdt sig til uddannelsens sammensætning; om det faglige indhold er relevant, og om der er faglige kompetencer, der bør styrkes eller mangler i uddannelsen.

Nedenstående viser en oversigt over i hvor høj grad aftagerne finder uddannelsesudkastet passende til de opgaver, der skal løses i virksomheden, så en virksomhed vil sende en medarbejder på masteruddannelsen i cybersikkerhed og risikohåndtering på SDU i Odense:

Aftagere	I høj grad	I mindre grad	Slet ikke
Fire Eater	X		
Terma	X		
KFISCH, DIIS og forsvarsministeriet	X		
Dansk Gummi Industri	X		
Gomspace	X		
Rambøll	X		
Sparrow Quantum	X		
Digital Frontier	X		
Orifarm	X		
Odense Kommune	X		
Jeros	X		
Dansk Sintermetal	X		
HMK Bilcon	X		
Unik Systemdesign	X		
Energinet	X		
Bankdata	X		

I nedenstående fremhæves aftagernes perspektiver og nuancer på uddannelsens indhold og sammensætning, herunder hvilke faglige kompetencer, der bør styrkes eller er vurderet som særligt vigtige:

Uddannelsesudkastet er rigtig godt sammensat - Fire Eater

Uddannelsens fokus skal være på at imødekomme, hvor gappet og manglerne er inden for områdets uddannelsesmuligheder. Jeg ser et særligt behov for medarbejdere, der kan arbejde med risiko i relation til operations-teknologi, eksempelvis udføre risikovurderinger i forhold til ISO og CIS. Det relaterer sig til de to fag på 2. semester. Det er vigtigt at fremhæve, hvilke konkrete værktøjer en studerende får med sig - Terma

I skal hjælpe disse nøglepersoner med at blive dygtige kommunikatører, der kan kommunikere modtagerorienteret både internt og eksternt i organisationen i krisesammenhænge. I har gavn af at fremhæve det mere forebyggende aspekt på uddannelsen. På første semester, under introduktionen til strategisk organisering, kan I med fordel understrege, at den studerende lærer at bidrage strategisk til ledelsen. På andet semester er det vigtigt at fokusere på, hvem der er fjender, med en grundlæggende forståelse af trusler, for eksempel hackere, stater, kriminelle og interne trusler samt sårbarheder. På fjerde semester vil jeg fremhæve, at masteropgaven fokuserer på en problematik i egen virksomhed, og overveje, om det er en faglig professionel opgave frem for en videnskabelig undersøgelse - KFISCH, DIIS og forsvarsministeriet

Fokus på risiko er vigtigt, hvilket fremgår af andet semester, men det hænger også tæt sammen med at lære at kommunikere dette. Fokus på at kunne vurdere fordele og ulemper ved de forskellige rammeværktøjer er også vigtigt, fx ISO 27001 og NIS2. Et fælles sprog for dette er vigtigt. Det vil være meget gavnligt at inddrage noget om awareness-træning i egen virksomhed i forhold til at mindske de interne trusler - Dansk Gummi Industri

For os er det vigtigt, at man på uddannelsen også forholder sig til konkrete værktøjer, som NIS2. Det er vigtigt at kunne navigere i systemerne og være systemspecifik. Vi er meget tool-specifikke - Gomspace

De fleste vil nok have en teknisk baggrund, og for dem vil det give mening at vælge fag fra ”Organisation” på 1. semester. 3. semester er meget relevant, bortset fra faget "Etik og Privathed," som ligger lidt uden for. Det er oplagt at anvende en case fra egen virksomhed i masteropgaven, da det også gør det mere attraktivt for virksomheden - Rambøll

Kombinationen af risikohåndtering, forretningskontinuitet og resiliens gør denne uddannelse særlig interessant og relevant. At lære at analysere og strukturere virksomhedens risici samt fokusere på de vigtigste risici er meget vigtigt. Det er også vigtigt at finde en god balance, da man aldrig vil kunne gøre det perfekt - Sparrow Quantum

Uddannelsen har et godt indhold og er virkelig interessant - Digital Frontier

Risikostyring, databeskyttelse og infrastruktur er særligt relevante for os - Orifarm

Det er vigtigt, at man får nogle værktøjer med hjem, for eksempel at kunne arbejde med NIS2 og risikohåndtering, at man kan forholde sig til de regler og regulativer, der løbende kommer, og at man kan omsætte det ved for eksempel at kunne anvende passende skabeloner - Odense Kommune

Det er vigtigt at få en forståelse af kompleksiteten ved cybersikkerhed, risikohåndtering og infrastrukturen - Jeros

Indholdet ser interessant ud. Værktøjer, man kan tage med hjem og omsætte, ville være interessante for os - Dansk Sintermetal

Pensummet er meget relevant. Jeg tænker, at man skal have en vis IT-interesse eller erfaring for at kunne følge med. Det er rigtig vigtigt, at uddannelsen indeholder noget med forsvar i dybden. Det ligger måske allerede i uddannelsen, men det vil være vigtigt at have kernekompetencer inden for dette område, altså informationssikkerhed, fysisk sikkerhed, sikkerhed i forhold til adgang til brugersystemer og generel awareness - HMK Bilcon

Det er særligt vigtigt at forbinde standarder med konkrete krav, for eksempel CIS18 med ISO-standarder, samt evnen til at omsætte dem til praktisk anvendelse. På uddannelsen er det meget vigtigt at fremhæve, hvorfor IT-sikkerhed er vigtig, da der er relativt lidt fokus på IT-sikkerhed i IT-uddannelser generelt. Faktisk er der få, der har kompetencerne til at løfte denne opgave. Det er også vigtigt at kunne inddrage IT-sikkerhed i ledelsesopbakning og forankring på bestyrelsesniveau samt kunne synliggøre omkostningerne ved valg og fravalg af forskellige risici - Unik Systemdesign

Det er de helt rigtige fagelementer, der er inkluderet i uddannelsen, men pas på at den ikke bliver for bred, da næsten alle fagelementerne i sig selv udgør en hel uddannelse. Det er vigtigt, at man kender til relevante IT-systemer på forhånd - Energinet

Det er et meget relevant indhold, især, computernetværk og cloud computing, principper for cybersikkerhed og resiliens i forsyningskæden. Men er det ikke en forudsætning, at man har hjemme i relevante IT-systemer? Alt på andet semester er relevant. Trusselsmodellering og risikostyring kunne også være et selvstændigt fag på 1. semester, da det udgør det grundlæggende fundament. Sikkerhedsarkitekturer er på et højt niveau, og det kræver, at man kan og har styr på det mere grundlæggende. 3. semester. Intelligens og Foresight, her er indsamlingsdelen ikke interessant, det svære og vigtige er at lære at analysere det. Anvendt cybersikkerhed er meget relevant, det er også Secure Software Operations, men det kunne ligge på en selvstændig kandidatuddannelse. Det er så grundlæggende vigtigt og afgørende, at man skal kunne det - Bankdata

Delkonklusion om hvilke kompetencer aftagerne fremhæver bør styrkes eller er særligt vigtige

- **Uddannelsens indhold og sammensætning er ambitiøs og relevant for virksomhederne**
  Aftagerne finder det faglige indhold og sammensætningen af uddannelsen ambitiøs og meget relevant. De har forskellige vægtninger af, hvilke fagelementer de vurderer som særlig betydningsfulde for deres virksomhed. De samlede og udtrykte betydningsfulde fagelementer er fremhævet nedenfor, og disse er allerede en del af uddannelsens indhold:
  Risikostyring med fokus på til- og fravalg samt en grundlæggende forståelse af trusler og IT-sikkerhed, herunder det forebyggende aspekt i arbejdet med risici.
  Evnen til at vurdere, omsætte og forbinde konkrete rammeværktøjer med ISO-standarder (NIS2, CIS, CIS18) til egen praksis i virksomheden.
  Et generelt fokus på læring og forståelse af kompleksiteten inden for cybersikkerhed og risikohåndtering, herunder infrastruktur og databeskyttelse.

Rollen som kommunikatør i relation til risici, awareness og sikkerhed bredt i virksomheden samt på strategisk niveau.

Konkret fremhæves følgende kurser på uddannelsen som særligt vigtige og interessante for virksomhederne: computernetværk og cloud computing, principper for cybersikkerhed og resiliens i forsyningskæden, forbedret trusselmodellering og risikostyring, virksomhedens sikkerhedsarkitektur, anvendt cybersikkerhed og software operations.

Aftagerne fremhæver desuden, at det er en styrke, at den afsluttende masteropgave målrettes en problemstilling i egen virksomhed.

I nedenstående fremhæves aftagernes perspektiver og nuancer på uddannelsens sammensætning og indhold, herunder hvilke nye faglige perspektiver de ser, vil tilføre yderligere værdi til uddannelsen:

Det er rigtig vigtigt og givende for nøglepersonerne, der har taget denne uddannelse, at de får et efterfølgende fagligt netværk, som kan være med til at fremme kontinuiteten i arbejdet med cybersikkerhed. Eksempelvis kan dette netværk afholde ét årligt møde sammen med universitetet - KFISCH, DIIS og forsvarsministeriet

Det er meget vigtigt at holde sig orienteret løbende, for eksempel via et netværk eller en vejledning i, hvor man kan følge med i de nyeste trends og generelt holde sig opdateret om områdets udvikling - Dansk Gummi Industri

For at sikre den læringsmæssige kontinuitet kunne man arbejde med at etablere et netværk, hvor man for eksempel samles og deler viden i en kombination mellem erhvervsliv og akademia - Digital Frontier

Det er vigtigt, at man lærer, at området vil kræve en løbende læring, så man løbende forbliver relevant og opdateret. Måske kunne et fagligt forum i en eller anden grad indgå eller være en del af uddannelsen - Odense Kommune

Delkonklusion om hvilke nye perspektiver aftagerne mener vil tilføre mere værdi til uddannelsen

- **Etablering af et fagligt netværk**
  Flere af aftagerne anbefaler etablering af et vedvarende fagligt netværk, der sikrer kontinuerlig læring samt løbende mulighed for at følge områdets udvikling.

I nedenstående har aftagerne forholdt sig til om der er andre aspekter SDU bør være opmærksomme på i forbindelse med oprettelsen af masteruddannelsen i cybersikkerhed og risikohåndtering:

Kommunikation om og forventninger til de praktiske forhold er vigtige at beskrive meget tydeligt, fx hvor mange dage om ugen, hvor mange sider der skal læses om ugen, hvor mange opgaver der skal laves, og den forventede tid der skal afsættes til opgaverne. Det er også vigtigt at informere om muligheder for online deltagelse og lignende. Jeres formidling af uddannelsens udbytte er meget vigtig - Fire Eater

Det er meget vigtigt at kommunikere tydeligt, hvilke praktiske muligheder den studerende har - Terma

Det praktiske og logistiske er vigtigt at fremhæve og præcisere i denne type uddannelse, hvor medarbejderen også skal arbejde ved siden af, især hvis undervisningen griber ind i hverdagen - Rambøll

Selvom uddannelsen er meget relevant, så vil I få modstand, da en masteruddannelse er svær at sælge, fordi virksomhederne skal betale. Det skal I være meget bevidste om, så I skal have ekstra fokus på markedsføringsdelen, og I skal lægge vægt på, hvad virksomhederne får ud af det. De skal kunne se, at det er en investering og ikke en udgift - Digital Frontier

I skal være opmærksomme på formen og formidlingen af uddannelsen, herunder de praktiske aspekter og, hvad man kan forvente. Det bør være obligatorisk for alle forretningsdrivende at have et "kørekort" til, hvordan man behandler personlige oplysninger - HMK Bilcon

Det kommunikative er vigtigt, så I gør det nemmere for os virksomheder og de studerende at forstå, hvorfor vi skal vælge jer - Bankdata

Delkonklusion om hvilke andre perspektiver SDU bør være opmærksomme på

- **Fokus på formidlingen af gevinsten ved at gennemføre uddannelsen samt på uddannelsens praktiske forhold**
  Flere af aftagerne anbefaler et øget fokus på formidlingen af uddannelsen, herunder forventninger til de praktiske og logiske forhold undervejs på uddannelsen, såsom hyppigheden af fremmøde, det forventede antal opgaver og den tid, der skal afsættes for at kunne følge uddannelsen. Derudover bør der lægges særlig vægt på formidlingen af gevinsten ved at gennemføre uddannelsen.

De samlede perspektiver er opsummeret i konklusionen på side 8. Forskningsmiljøets revision af uddannelsens indhold efter aftagernes anbefalinger kan læses på side 9.

Støtteerklæringer

Støtteerklæringer til masteruddannelsen i cybersikkerhed og risikohåndtering på SDU i Odense:

Kristian Fischer ejer af KFISCH, tidligere direktør i DIIS og tidligere en del af forsvarsministeriets ledelse
Med baggrund i mit arbejde i og med store, videnstunge, fagprofessionelle, offentlige organisationer er jeg overbevist om, at den planlagte SDU-uddannelse vil være særdeles efterspurgt. Den vil være med til substantielt at udvikle allerede "forretningskritiske" professionelle funktioner samt bidrage til at opbygge faglige netværk til gavn for såvel organisationer, virksomheder samt deres medarbejdere.

Dansk Gummi Industri
Masteruddannelsen i cybersikkerhed og risikohåndtering er et fantastisk initiativ, som vi støtter 100% op om. Uddannelsens bredde og muligheder i kombination med vigtigheden af at fokusere på læring af konkrete værktøjer, som eksempelvis rammeværktøjer, er superrelevant og vi SMV'er savner et fælles sprog så vi slipper for hver især at opfinde den dybe tallerken – eller være 100% i lommen på konsulenter. Det vil gavne vores konkurrenceevne markant og vi vil helt sikkert sende folk afsted på uddannelsen, når den forhåbentligt kommer.

Rambøll
Vi støtter uddannelsen i cybersikkerhed og risikohåndtering på Syddansk Universitet i Odense. Uddannelsen starter på et særdeles relevant tidspunkt og indeholder de væsentligste fagelementer, som vil give virksomhederne de rette faglige kompetencer til at sikre sig digitalt.

Unik Systemdesign
Denne uddannelse er relevant for virksomheder som vores, fordi vi blandt andet bliver indirekte omfattet af NIS2, hvor risikohåndtering er en stor del af det. Vi har ikke haft et stort fokus på IT-sikkerhed, og denne uddannelse repræsenterer en struktureret tilgang til området. Med udgangspunkt i risici, og dermed potentielle omkostninger, er det en parameter de fleste ledere kan forholde sig til, også dem uden den store tekniske indsigt. Behovet for at kunne snakke det "organisatoriske sprog", og oversætte til og fra et IT-sikkerhedsteknisk sprog er yderst relevant.

Technology Denmark
Technology Denmark støtter oprettelsen af en masteruddannelse i cybersikkerhed og risikohåndtering ved Syddansk Universitet som følge af det stigende trusselbillede og de tilhørende øgede lovkrav inden for cybersikkerhed. Dette kræver løbende opkvalificering og kompetenceudvikling i erhvervslivet, så virksomheder kan håndtere de komplekse sikkerhedsudfordringer og trusler, de står overfor.

Erhvervshus Fyn
Erhvervshus Fyn støtter oprettelsen af masteruddannelsen i cybersikkerhed og risikohåndtering ved Syddansk Universitet i Odense. Vi finder uddannelsen relevant set i lyset af de stigende lovgivningskrav og det øgede trusselsbillede inden for cybersikkerhed. Uddannelsen kan medvirke til at styrke virksomhedernes kompetencer, så de kan forbedre deres digitale sikkerhed og forblive konkurrencedygtige.

Referencer

1.) National strategi for cyber- og informationssikkerhed 2022-2024 [(1)]. https://fm.dk/media/rgm-chosw/national-strategi-for-cyber-og-informationssikkerhed_web-a.pdf [(1)].

2.) Barometerundersøgelsen 2024 [(2)]. https://itb.dk/nyheder/her-er-branchens-stoerste-vaekstbarrierer-for-2024/ https://docs.google.com/presentation/d/1wpByDFix11Nw1X5ENGbLQoqIn-LhC8CYl/edit?slide=id.p1#slide=id.p1.

3.) Cybersikkerhed i små og mellemstore danske produktionsvirksomheder 2024 [(3)]. https://findre-searcher.sdu.dk/ws/portalfiles/portal/265031161/Cybersikkerhed_i_smaa_og_mellemstore_danske_produktionsvirksomheder.pdf

4.) Digital sikkerhed i danske SMV'er 2024 [(4)]. https://digst.dk/media/hskb5hdp/digital-sikkerhed-i-danske-smver-2023_endelig0310-a.pdf

5.) SDU's aftagerundersøgelse (2025).

6.) Støtteerklæringer fra relevante aftagere (2025).

Det Naturvidenskabelige Fakultet

Det Samfundsvidenskabelige Fakultet

10. September 2025

Sabine Hildebrand
sabh@sdu.dk

Følgebrev til ansøgning om prækvalifikation af ny masteruddannelse i cybersikkerhed og risikohåndtering

Syddansk Universitet (SDU) fremsender hermed ansøgning om prækvalifikation af en ny masteruddannelse i cybersikkerhed og risikohåndtering, forankret på Det Naturvidenskabelige Fakultet. Uddannelsen er udviklet i tæt samarbejde med fagmiljøet bag SDU's relaterede masteruddannelse i intelligence- og cyberstudier, som har været udbudt af Det Samfundsvidenskabelige Fakultet siden 2021.

Den nye masteruddannelse i cybersikkerhed og risikohåndtering adresserer nye behov for et tværfagligt fokus, der kombinerer læring inden for cybersikkerhed, IT-governance og forretningsstyring. Den giver nøglepersoner strategiske og operationelle kompetencer til at integrere cyber- og forretningsrisici i virksomheders sikkerhedsarkitektur og forretningsstrategier. Uddannelsen er målrettet erhvervslivet og understøtter implementering af cybersikkerhed, der balancerer tekniske, organisatoriske og juridiske hensyn.

Den eksisterende masteruddannelse i intelligence og cyberstudier ruster de studerende til et foranderligt trusselsbillede, hvor cyber- og intelligence-spørgsmål i stigende grad præger vores daglige arbejds- og beslutningsprocesser. Uddannelsen, der udbydes i samarbejde med Forsvarsakademiet, bidrager til området med indsigt i, hvordan stater og virksomheder arbejder strategisk for at beskytte sig mod cybertrusler fra it-kriminelle og fremmede magter, og den er målrettet analytikere, specialister og beslutningstagere i Forsvaret, Politiet, forvaltningen eller fx forsikringsbranchen.

Med to forskellige målgrupper er de to masteruddannelser komplementære, men bygger på fælles forskning, blandt andet i regi af forskningsprojektet, Cybersikkerhed og Forretningskontinuitet, hvor en bred kreds af danske virksomheder deltager. Dette forsknings- og erhvervsrettede samarbejde har i det forgangne år tydeliggjort et stigende behov for efter- og videreuddannelse med en ny kombination af kompetencer inden for cybersikkerhed og risikohåndtering, målrettet nøglepersoner med ansvar for digital sikkerhed i danske virksomheder og organisationer. Tilsvarende behov er efterfølgende underbygget i arbejdsmarkedsbehovsundersøgelse tilknyttet den ansøgte uddannelse.

Sammen vil de to masteruddannelser styrke Danmarks digitale robusthed ved at dække både de samfundsmæssige og forretningsmæssige dimensioner af cybersikkerhed. Uddannelserne bidrager til at imødekomme nationale og internationale regulatoriske krav og understøtter den nationale strategi for cyber- og informationssikkerhed. SDU ser gode muligheder for samspil og synergi mellem forskning, de to uddannelser og det omgivende samfund inden for dette felt.

Med venlig hilsen

Helle Waagepetersen
Prorektor ved SDU

Syddansk Universitet
Campusvej 55
5230 Odense M
T +45 6550 1000
www.sdu.dk

Uddannelses- og Forskningsministeriet

Syddansk Universitet
Rektor Jens Ringsmose

Kære Jens Ringsmose

På baggrund af gennemført prækvalifikation af Syddansk Universitets ansøgning om godkendelse af ny uddannelse er der truffet følgende afgørelse:

Godkendelse af ny masteruddannelse i cybersikkerhed og risikohåndtering (Odense)

Afgørelsen er truffet i medfør af § 23, stk. 1, nr. 1 i bekendtgørelse om akkreditering af videregående uddannelsesinstitutioner og godkendelse af videregående uddannelser (nr. 820 af 23. juni 2025).

Det er en forudsætning for godkendelsen, at uddannelsen og dennes studieordning opfylder uddannelsesreglerne, herunder bekendtgørelse nr. 19 af 9. januar 2020 om masteruddannelser ved universiteterne og bekendtgørelse nr. 2272 af 1. december 2021 om universitetsuddannelser tilrettelagt på deltid med senere ændringer.

Da Syddansk Universitet er positivt institutionsakkrediteret, gives godkendelsen til umiddelbar oprettelse af uddannelsen.

Udbudsgodkendelsen kan bortfalde efter § 15 h i lov om videregående uddannelse (videreuddannelsessystemet) for voksne, jf. lovbekendtgørelse nr. 1038 af 30. august 2017.

Ansøgningen er blevet vurderet af Det rådgivende udvalg for vurdering af udbud af videregående uddannelser (RUVU). Vurderingen er vedlagt som bilag.

Vedlagt i bilag er desuden uddannelsens grundoplysninger. Ved spørgsmål til afgørelsen eller de vedlagte grundoplysninger kan Uddannelses- og Forskningsstyrelsen kontaktes på pkf@ufm.dk.

Med venlig hilsen

Christina Egelund

Bilag: 1 – RUVU's vurdering af ansøgningen
2 – Følgebrev fra Uddannelses- og Forskningsstyrelsen med uddannelsens grundoplysninger

17. november 2025

Uddannelses- og Forskningsministeriet

Bredgade 40-42
1260 København K

Tel. 3392 9700
ufm@ufm.dk
www.ufm.dk

CVR-nr. 1680 5408

Ref.-nr.
2025 - 55198

Bilag 1 – RUVU's vurdering af ansøgningen

Nr. A1 – ny uddannelse (Efterår 2025)			**Status på ansøgningen:** Godkendt	
Ansøger og udbudssted:	Syddansk Universitet (Odense)			
Uddannelsestype:	Masteruddannelse			
Uddannelsens navn (fagbetegnelse) på hhv. dansk/engelsk:	- Cybersikkerhed og risikohåndtering - Cybersecurity and Risk Management			
Betegnelse, som uddannelsen giver ret til at anvende:	- Master i cybersikkerhed og risikohåndtering - Master of Cybersecurity and Risk Management			
Hovedområde:	Naturvidenskab		**Genansøgning:**	Nej
Sprog:	Dansk	**Antal ECTS:**	60 ECTS	
Link til ansøgning på pkf.ufm.dk:	https://pkf.ufm.dk/flows/7313cea543d8f65110a9c715d479fdc7			
RUVU's vurdering	RUVU vurderer, at ansøgningen ***opfylder*** kriterierne som fastsat i bekendtgørelsen. RUVU lægger vægt på, at ansøgningen dokumenterer et aktuelt behov efter uddannelsens dimittender samt en efterspørgsel hos lokale virksomheder efter at sende deres medarbejdere på videreuddannelse inden for cybersikkerhed og risikohåndtering. RUVU finder det godtgjort, at uddannelsen ikke vil have negativ indvirkning på konkurrerende tilbud. RUVU finder det også positivt, at uddannelsen kan være med til at løfte uddannelsesniveauet hos IT-professionelle uden formel uddannelse, der har behov for relevant opkvalificering.			

Bilag 2 – Følgebrev fra Uddannelses- og Forskningsstyrelsen med uddannelsens grundoplysninger

Masteruddannelsen i cybersikkerhed og risikohåndtering
Master of Cybersecurity and Risk Management

Hovedområde:
Naturvidenskab

Betegnelse:
Efter reglerne i § 5, stk. 1, i bekendtgørelse nr. 19 af 9. januar 2020 om masteruddannelser ved universiteterne (masterbekendtgørelsen), giver uddannelsen ret til betegnelsen:

- **Dansk:** Master i cybersikkerhed og risikohåndtering
- **Engelsk:** Master of Cybersecurity and Risk Management

Udbudssted:
Odense

Sprog:
Dansk

Normeret studietid:
Efter reglerne i masterbekendtgørelsens § 6, stk. 2, fastlægges uddannelsens normering til 60 ECTS-point.

Takstindplacering:
Uddannelsen indplaceres til: Deltidstakst 2
Aktivitetsgruppekode: 5969

Koder Danmarks Statistik:
UDD: 8590
AUDD: 8590

Censorkorps
Ministeriet har noteret sig, at uddannelsen tilknyttes censorkorps for datalogi.

Adgangskrav
Efter det oplyste er følgende adgangskrav jf. § 9 i masterbekendtgørelsen gældende:

- En relevant kandidat-, bachelor-, professionsbachelor- eller tilsvarende diplomuddannelse fra en videregående uddannelsesinstitution, der giver grundlæggende viden inden for mindst ét af følgende områder: Datalogi, softwareudvikling, informationsteknologi, IT-arkitektur, erhvervsøkonomi, ledelse, økonomi, organisationsstudier, jura, kommunikation eller samfundsvidenskab.
- Ansøgerne skal efter gennemført adgangsgivende uddannelse have mindst to års relevant erhvervserfaring inden for mindst ét af følgende områder:

Softwareudvikling, systemadministration, IT-drift, IT-sikkerhed, datagovernance, regulatorisk compliance, organisatorisk styring, projektledelse, risikostyring eller administration.

Bilag 2 – Følgebrev fra Uddannelses- og Forskningsstyrelsen med uddannelsens grundoplysninger (revideret 5. maj 2026)

Masteruddannelsen i cybersikkerhed og risikohåndtering
Master of Cybersecurity and Risk Management

Hovedområde:
Naturvidenskab

Betegnelse:
Efter reglerne i § 5, stk. 1, i bekendtgørelse nr. 19 af 9. januar 2020 om masteruddannelser ved universiteterne (masterbekendtgørelsen), giver uddannelsen ret til betegnelsen:

- **Dansk:** Master i cybersikkerhed og risikohåndtering
- **Engelsk:** Master of Cybersecurity and Risk Management

Udbudssted:
Odense

Sprog:
Dansk

Normeret studietid:
Efter reglerne i masterbekendtgørelsens § 6, stk. 2, fastlægges uddannelsens normering til 60 ECTS-point.

Takstindplacering:
Uddannelsen indplaceres til: Deltidstakst 2
Aktivitetsgruppekode: 5969

Koder Danmarks Statistik:
UDD: 8968
AUDD: 8968

Censorkorps
Ministeriet har noteret sig, at uddannelsen tilknyttes censorkorps for datalogi.

Adgangskrav
Efter det oplyste er følgende adgangskrav jf. § 9 i masterbekendtgørelsen gældende:

- En relevant kandidat-, bachelor-, professionsbachelor- eller tilsvarende diplomuddannelse fra en videregående uddannelsesinstitution, der giver grundlæggende viden inden for mindst ét af følgende områder: Datalogi, softwareudvikling, informationsteknologi, IT-arkitektur, erhvervsøkonomi, ledelse, økonomi, organisationsstudier, jura, kommunikation eller samfundsvidenskab.
- Ansøgerne skal efter gennemført adgangsgivende uddannelse have mindst to års relevant erhvervserfaring inden for mindst ét af følgende områder:

Softwareudvikling, systemadministration, IT-drift, IT-sikkerhed, datagovernance, regulatorisk compliance, organisatorisk styring, projektledelse, risikostyring eller administration.