Co-funded by the European Union

D3.1 OPPLÆRINGSMODULER FOR STUDENTER VED HØYERE UTDANNINGSINSTITUSJONER

CYBERAGENT 09.2025

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

Arbeidspakke 3: Utvikling av læringsressurser for cyberagenter

Leveranse 3.1: Opplæringsmoduler for studenter ved høyere utdanningsinstitusjoner

Leder av WP3 – TIMTAL. Leder av D3.1 – VU.

INNHOLD

INNLEDNING 2

1. M1: SIKKERHETSPROGRAMADMINISTRASJON 4
2. M2: SYSTEMADMINISTRASJON 8
3. M3: ANALYTISKE VERKTØY 15
4. M4: SIKKERHETSOPERASJONER 20
5. M5: SIKKERHETSSTYRING OG -POLITIKK 24
6. M6: PLANLEGGING AV CYBERSIKKERHET 31
7. M7: RISIKOSTYRING OG RISIKOMINIMERING 33
8. M8: FORRETNINGSKONTINUITET, KATASTROFEGENOPPRETTING, HENDELSESHÅNDTERING OG PERSONALSIKKERHET 40

VEDLEGG 46

MAL FOR SYLLABUS 46

INNLEDNING

Ifølge D2.2-rapporten står SMB-bedrifter overfor en betydelig mangel på kvalifiserte cybersikkerhetsspesialister, og eksisterende ansatte mangler ofte den systemiske kunnskapen som kreves for å reagere hensiktsmessig på stadig mer komplekse cybertrusler. Derfor er det særlig viktig i høyere utdanning å utdanne spesialister som kan anvende sin kunnskap i SMB-miljøet – både på det tekniske og ledelsesmessige området. I lys av dette ble det i dokumentet D2.3 utarbeidet en kompetansebasert læringsvei, delt inn i ulike temaområder og med fokus på utvikling av praktiske ferdigheter.

Dette dokumentet presenterer et av hovedresultatene av prosjektet – opplæringsmodulene for studenter i høyere utdanning (D3.1). Målet med denne aktiviteten er å lage opplæringsplaner for høyere utdanningsinstitusjoner (HEI) som dekker de viktigste områdene av kunnskap, ferdigheter og kompetanse innen cybersikkerhet som er relevante for små og mellomstore bedrifter (SMB).

Disse modulene er resultatet av et konsekvent arbeid basert på en detaljert behovsanalyse (D2.2), hvor representanter fra SMB, yrkesrettet utdanning og opplæring (VET) og høyere utdanningsinstitusjoner ble undersøkt, samt en klart definert læringsløpsstruktur (D2.3).

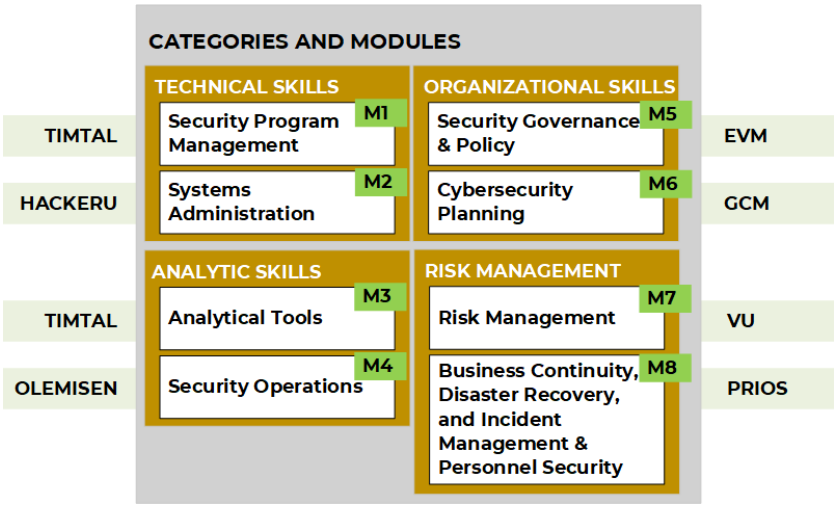
Opplæringsprogrammet, som tilsvarer nivå 5–6 i det europeiske kvalifikasjonsrammeverket (EQF), er utformet for studenter i høyere utdanning og avanserte SMB-ansatte. Det består av åtte kjernemoduler og en inspirerende modul, som dekker fire viktige kompetanseområder:

- **Tekniske ferdigheter** (sikkerhetsprogramadministrasjon, systemadministrasjon).
- **Analytiske ferdigheter** (analytiske verktøy, sikkerhetsoperasjoner).
- **Organisatoriske ferdigheter** (sikkerhetsstyring og -politikk, planlegging av cybersikkerhet).
- **Risikostyring** (risikostyring og -begrensning, forretningskontinuitet, katastrofegjenoppretting og hendelseshåndtering og personellsikkerhet).

Hver modul er verdt 3 ECTS-poeng (tilsvarende 75 timers studentarbeid), er i tråd med prinsippene for høyere utdanning og følger metodiske anbefalinger spesifisert i D2.3: utdanningen er basert på aktive læringsmetoder (f.eks. casestudier, prosjektbasert læring) og selvstyrt læring, med læringsutbytte som er tydelig skilt mellom nivåene kunnskap, ferdigheter og kompetanse.

Hver modul på 3 ECTS-poeng er utviklet av forskjellige konsortiepartnere, som har utnyttet sin spesifikke faglige og profesjonelle erfaring.

De utviklede modulene dekker følgende nøkkelområder, som er identifisert som kritisk viktige i D2.2-rapporten:



1. M1: SIKKERHETSPROGRAMLEDELSE

Modultittel	Modulens kode
SIKKERHETSPROGRAMLEDELSE	

Foreleser(e)	Institusjon eller avdeling hvor modulen undervises

Undervisningsform	Språk
Ansikt til ansikt, online, hybrid	*Engelsk, finsk, tyrkisk, norsk, litauisk, rumensk, fransk, polsk, spansk*

Forutsetninger
Ingen

Antall tildelte ECTS-poeng	Studentens arbeidsbelastning	Kontaktarbeidstimer	Individuelle arbeidstimer
3	75 timer	50 timer	25 timer

Formål og resultater av modulen		
Etter å ha fullført dette kurset vil studentene ha tilegnet seg ferdigheter til å effektivt administrere sikkerhetsprogrammer som svar på cybersikkerhetstrusler. De vil utvikle forsvarsstrategier mot aktuelle trusler som phishing, ransomware og DDoS-angrep innenfor rammen av prosjekt- og ressursadministrasjon. I tillegg vil studentene lære å anvende sikkerhetsmålinger og kvalitetssikringsmetoder, og få evnen til å optimalisere sikkerhetsprogrammer, administrere ressurser effektivt og forbedre organisasjonens sikkerhet ved å bruke passende verktøy mot nye trusler. Dette kurset vil også bygge opp deres kompetanse innen trusselvurdering, rapportering og kommunikasjon, slik at de kan implementere cybersikkerhetsstrategier effektivt i sine organisasjoner.		
Læringsutbytte av modulen	**Undervisnings- og læringsmetoder**	**Vurderingsmetoder**
Kunnskap: Studentene vil tilegne seg praktisk kunnskap om de nyeste cybersikkerhetstruslene, inkludert phishing, ransomware og DDoS-angrep, og hvordan de kan håndtere disse gjennom effektiv prosjekt- og ressursstyring og implementering av kvalitetssikrings- og kontrolltiltak.	Velges av foreleseren fra del 1.3. [Undervisningsmetoder, f.eks. teoretiske forelesninger, gjesteforelesere, quizzer, spill, praktiske oppgaver/laboratorier, peer-to-peer-undervisning og -læring, selvstyrt læring osv.	Selvtest Kunnskapsvurderingstest

Ferdigheter: Lærerne vil være i stand til å bruke verktøy og programvare for beskyttelse mot stadig nye cybertrusler, og anvende robuste sikkerhetsrutiner i prosjekt- og ressursstyring for å forbedre de samlede sikkerhetsmålene og kvalitetskontrollen i sine organisasjoner.	Velges av foreleseren fra del 1.3. [Undervisningsmetoder, f.eks. praktiske oppgaver/laboratorier, praktiske aktiviteter, simulerte miljøer, spørrekonkurranser, spill, casestudier osv.] i D2.3 «Strukturen i læringsløpet for SMB-cybersikkerhetsagenter»	Praktiske vurderinger
Kompetanse: Lærerne skal være kompetente i å vurdere og redusere potensielle sikkerhetstrusler, kommunisere cybersikkerhetsproblemer på en effektiv måte og rapportere trusler og brudd nøyaktig gjennom de riktige kanalene i organisasjonen.	Velges av foreleseren, fra del 1.3. [Undervisningsmetoder, f.eks. simulerte miljøer, capture the flag-konkurranser, 5E, CBL, CL, POGIL, PBL osv.] i D2.3 «Strukturen i læringsløpet for SMB-endringsagenter innen cybersikkerhet»	Simuleringer Konkurranser

Modulens innhold: oversikt over emnene	**Kontaktarbeidstimer**					**Individuelle arbeidstimer og oppgaver**	
	Forelesninger (HEI)	Konsultasjoner	Praksis (HEI)	Tester	**Alt**	**Individuelt**	**Oppgaver**
Prosjektledelse • Prosjektplanlegging • Definere prosjektmål • Definere prosjektomfang og krav • Utarbeide prosjektplan • Prosjektledelsesverktøy • Aktuelle cybersikkerhetstrusler (DDoS, løsepengevirus, skadelig programvare, phishing, zero-day, IoT-angrep osv. • Trusselmodellering og sårbarhetsanalyse • Nød- og hendelsesresponsplaner • Rapportering av cybersikkerhetstrusler og hendelser	8	0,5	3	0,5	**12**	**6**	• Planlegg et prosjekt for å øke bevisstheten om cybersikkerhet blant ansatte i små og mellomstore bedrifter. • Definer klare mål for prosjektet for å øke SMB-ansattes bevissthet om cybersikkerhet, slik at de får bedre forståelse for potensielle sikkerhetstrusler. • Skissere omfanget og kravene til prosjektet for å øke bevisstheten om cybersikkerhet blant ansatte i små og mellomstore bedrifter, inkludert opplæringstemaer og nødvendige ressurser.

							• Utarbeid tidsplanen for prosjektet for å øke SMB-ansattes bevissthet om cybersikkerhet. • Bruk prosjektledelsesverktøy for å overvåke fremdriften og ressursutnyttelsen for prosjektet for å øke bevisstheten om cybersikkerhet blant ansatte i små og mellomstore bedrifter. • Undersøk aktuelle cybersikkerhetstrusler og samle funnene i en rapport. • Lag en forenklet trusselmodell for å hjelpe SMB-ansatte med å identifisere potensielle sikkerhetsproblemer i deres daglige drift. • Finn og gjennomgå eksempler på beredskaps- og hendelsesresponsplaner. • Hvilke trinn bør vurderes når man utarbeider en rapport om rapportering av cybersikkerhetstrusler og hendelser? Undersøk og oppsummer.
Ressursstyring • Personaladministrasjon (prosjektgrupper) • Sikkerhetsbevissthet og teamopplæring • Inventarstyring av maskinvare og programvare • Sikkerhetsverktøy og programvare • Effektiv bruk av teknologiske ressurser • Budsjett og ressursfordeling	8	0,5	3	0,5	**12**	**6**	• Planlegg en ressursstyringsstrategi for å sikre effektiv ressursbruk for en fiktiv SMB. • Lag et eksempel på en emneplan for opplæring i cybersikkerhet. • Utarbeid en oversikt over maskinvare og programvare for en fiktiv SMB. • Undersøk vanlige sikkerhetsverktøy og programvare.

							• Lag et eksempel på et budsjett og en ressursfordelingsplan for en hypotetisk SMB.
Sikkerhetsmålinger • Sikkerhetsmetrikker og målingsteknikker • Datainnsamling med SIEM • Analyse av sikkerhetsmetrikker • Prosjektoppfølging og ytelsesevaluering • Gjennomgang av tiltak og prosjekt tilpasning • Rapportering av sikkerhetsmetrikker	8	0,5	4	0,5	**13**	**6**	• Undersøk sikkerhetsmetrikken som brukes til å vurdere cybersikkerheten i små og mellomstore bedrifter. • Undersøk kildene som SIEM-programvaren henter logger fra. • Konfigurer og undersøk en åpen kildekode-SIEM-programvare. • Analyser sikkerhetsmetrikker ved å samle inn logger ved hjelp av SIEM-programvare. • Rapporter analyseresultatene av sikkerhetsmetrikker med grafer og visuelle fremstillinger.
Kvalitetssikring og kvalitetskontroll • Kvalitetsstyring • Kvalitetsstandarder innen cybersikkerhet • Overholdelse og kvalitetsrevisjoner • Testing og valideringsteknikker • Evaluering og forbedringsanbefalinger	8	0,5	4	0,5	**13**	**7**	• Hvordan bør kvalitetssikrings- og kvalitetskontrollprosesser planlegges for å øke effektiviteten av cybersikkerhetsapplikasjoner i små og mellomstore bedrifter? Undersøk og oppsummer. • Undersøk kontrollpunktene i vedlegg A til ISO/IEC 27001:2022. • Undersøk og rapporter om hva test- og valideringsteknikker er. • Hvilke fordeler gir kontinuerlig gjennomgang og forbedring av kvalitetsprosesser for små og mellomstore bedrifter?
Totalt	**32**	**2**	**14**	**2**	**50**	**25**	

Vurderingsstrategi	Sammenlignende vektprosent	Vurderingskriterier
Selvtest I	10	10 poeng – 95–100 % riktige svar. 9 poeng – 85–94 % riktige svar. 8 poeng – 75–84 % riktige svar. 7 poeng – 65–74 % riktige svar. 6 poeng – 55–64 % riktige svar. 5 poeng – 45–54 % riktige svar. 4 poeng – 35–44 % riktige svar. 3 poeng – 25–34 % riktige svar. 2 poeng – 15–24 % riktige svar. 1 poeng – 0–14 % riktige svar.
Selvtest II	10	
Selvtest III	10	
Selvvalueringstest IV	10	
Kunnskapsvurderingstest	60	

Studiemateriale *(Etternavn, forbokstav. (År, måned, dag). Artikkelens tittel. Tidsskrift/journal/avisens tittel, volumnummer (utgavenummer), sidetall for hele artikkelen, utgiver, URL)*
Obligatorisk lesning
Anbefalt lesning
https://sansorg.egnyte.com/dl/RFrVIbX2oc https://edwps.com/wp-content/uploads/2018/04/Cyber-PMO-U.S.-Cyber-Magazine.pdf https://healthybyte.net/cybersecurity/what-is-a-security-program-management

2. M2: SYSTEMADMINISTRASJON

Modultittel	Modulnummer
SYSTEMADMINISTRASJON	

Foreleser(e)	Institusjon eller avdeling hvor modulen undervises

Undervisningsform	Språk
Ansikt til ansikt, online, blandet	*Engelsk, finsk, tyrkisk, norsk, litauisk, rumensk, fransk, polsk, spansk*

Forutsetninger
Ingen

Antall tildelte ECTS-poeng	Studentens arbeidsbelastning	Kontaktarbeidstimer	Individuelle arbeidstimer
3	75	5	25

Formål og læringsutbytte
Etter å ha fullført dette kurset vil studentene være i stand til å kontinuerlig håndtere (identifisere, analysere, vurdere, estimere, redusere) cybersikkerhetsrelaterte risikoer ved IKT-infrastrukturer, -systemer og -tjenester ved å planlegge, anvende, rapportere og kommunisere risikoanalyse, -vurdering og -behandling. Studentene vil lære grunnleggende nettverkskunnskap for å kunne administrere nettverksenheter på riktig måte, operere på både Linux- og Windows-servere og administrere og sikre dem. Kunnskap om sky og AI i sammenheng med cybersikkerhet vil også være svært nyttig for dem for å kunne øke hastigheten på oppgaver og utføre automatiseringer og skalering. Studentene vil også lære hvordan de kan sikre systemer, utføre trusseljakt og gjøre servere tilgjengelige (akronym fra CIA-triaden).

Læringsutbytte av modulen	Undervisnings- og læringsmetoder	Vurderingsmetoder
Kunnskap: Studentene vil tilegne seg kunnskap om nettverksadministrasjon, operativsystemer, grunnleggende nettverkskunnskap, verktøy for nettverksadministrasjon, sikkerhet for nettverksenheter, Linux-systemadministrasjon, Windows-systemadministrasjon, virtualisering, cloud computing ved bruk av AI for nettverks- og cybersikkerhetsprosedyrer, cybersikkerhetsprosedyrer, trusseloppdagelse, trusselanalyse, trusselrespons, trusselavhjælpning, grunnleggende cybersikkerhet, forsvar av organisasjonen mot angrep, infrastruktur- og nettverkssikkerhet, nettverksovervåking og -analyse, håndtering av hendelser. De vil være i stand til å etablere og beskrive effektive systemadministrasjonsprosedyrer og driftsrutiner tilpasset de spesifikke behovene til SMB-arbeidsplasser i samsvar med standarder.	Velges av foreleseren, live-undervisning, videoopptak, presentasjoner, virtuelle apparater (hvis aktuelt), litteraturanalyse, gjesteforelesere, peer-to-peer-undervisning og læring, veiledning.	Selvtest og kunnskapstest

Ferdigheter: Studentene vil være i stand til å bruke metodikker og verktøy for å designe og implementere sikre systemarkitekturer, inkludert operativsystemer, databaser, nettverk og skyinfrastrukturer for SMB-arbeidsplasser.	Velges av foreleseren: live-undervisning, videoopptak, presentasjoner, virtuelle apparater (hvis aktuelt), litteraturanalyse, gjesteforelesere, peer-to-peer-undervisning og læring, veiledning.	Selvvalueringstester og kunnskapstester
Kompetanse: Studentene vil være kompetente til å utvikle og implementere strategiske rammeverk for cybersikkerhet for systemadministrasjon, lede prosjekter og team for å forbedre systemets sikkerhet og tilgjengelighet, og ta etiske beslutninger for å opprettholde robuste cybersikkerhetsrutiner på tvers av ulike administrative domener for SMB-arbeidsplasser.	Velges av foreleseren, live-undervisning, videoopptak, presentasjoner, virtuelle apparater (hvis aktuelt), litteraturanalyse, gjesteforelesere, peer-to-peer-undervisning og læring, veiledning.	Selvtest og kunnskapstest

Modulens innhold: oversikt over emnene	**Kontakt arbeidstid**					**Individuelle arbeidstimer og oppgaver**	
	Forelesninger (HEI)	Konsultasjoner	Praksis (HEI)	Tester	**Alt**	**Individuelt arbeid**	**Oppgaver**
Operativsystemadministrasjon • Operativsystemer • Forholdet mellom maskinvare og programvare • Binære tall, heksadesimal telling • Biter og byte • Kommandolinje i operativsys-temet • Windows- og Linux-kommandoer • Windows-klient og -server • Programmer, prosesser og tjenes-ter i Windows • Filtyper og filformater • Registernøkler og verdier • Kontrollpanelinnstillinger	4	0,5	2	0,5	**7**	**3,5**	Heksadesimal telling Øve på Windows-kommandoer Øve på Linux-kommandoer Øvelse på oppgavebehandling Oppretting og administrering av filer Endring og visning av registertaster og -verdier Endring av kontrollpanelinnstillin ger Administrere brukere og grupper

• Brukere og grupper • Domenestruktur og serveradmin-istrator • AD og GPO • Linux-grensesnitt og kjernen • Prosesser i Linux • Navngivningskonvensjoner for filer og kataloger • Linux-skall og kommandosyntaks • Manipulering av filer og mapper • Arbeide med pipe og sys-temovervåkingskommandoer • Prosessadministrasjon og jobbkontroll • Tjenestestyring							Administrere domenestruktur Oppretting og sletting av Active Directory-objekter Administrere prosesser i Linux Manipulere filer og mapper Arbeide med pipe Systemovervåkingsko mmandoer Administrere Linux-tjenester
Administrasjon av databasesystemer • Repositorier og kildelister • Administrere en webserver • Systemlogger og loggovervåking • Planlegging av oppgaver i Linux • Feilsøking av server og nettverk • Sikkerhetskopiering og gjenop-pretting • Sikring av GRUB • Brannmurer • Active Directory-objekter og GPO-administrasjon • DNS og DHCP • Grunnleggende om PowerShell • Microsoft BitLocker, AppLocker og brannmur • LDAP og Kerberos • NTLM • Passord- og låsepolitikker • Autentisering og tilgangskontroll • Internet Control Message Protocol (ICMP) • TCP vs UDP • NetBIOS og SMB • SSL og TLS • Sertifikater • Telnet og Secure Shell (SSH) proto-koller • HTTP og HTTPS • E-postsystemprotokoller • Domain Name System Protocol (DNS) • FTP og RDP • Innkapsling vs. utkapsling • Nettverkssniffere og Wireshark • TCP/UDP • DHCP, DNS	4	0,5	2	0,5	**7**	**3,5**	Administrere arkiver og kildelister Administrere en webserver Verifisering og administrering av systemlogger og loggovervåking Planlegging av oppgaver i Linux Feilsøking av server Gjenoppretting av sikkerhetskopier Sikring av GRUB Administrere DB-tjenester Konfigurere passordpolicyer Konfigurere retningslinjer for kontosperring Konfigurere autentisering og tilgangskontroll

Nettverksadministrasjon • Nettverkstyper og trådløse nettverk • Nettverk og topologier • Enheter Identitet og tilgangsenheter • Infrastruktur og sikkerhetsenheter • Spesialiserte enheter og nettverksarkitektur • Virtuelle nettverk • Fysiske og logiske adresser • OSI og nettverksmodeller • Datakapsling og dekapsling • Nettverksprotokoller og portnumre • Nettverksmedier og kabler • Trådløse teknologier • Verktøy for nettverksadministrasjon • Cisco Packet Tracer • Nettverksklasser og undernett • Adresseresolusjonsprotokoll (ARP) • Statisk vs. dynamisk IP-adressering • Nettverksadresseoversettelse (NAT) • Switcher og Cisco IOS • Switches port sikkerhet og rutergrensesnitt • Konfigurering av VLAN-er og DTP • Ruting mellom VLAN-er • Introduksjon til ACL-er • Feilsøking i nettverk	4	0,5	2	0,5	**7**	**3,5**	Opprette nettverkstopologier Administrere nettverksenheter Bygg nettverket Sikring av nettverksenheter Opprette virtuelle nettverk Konfigurere nettverksprotokoller og portnumre Arbeide med Cisco Packet Tracer Arbeide med Address Resolution Protocol (ARP) Planlegge et nettverk Konfigurere statisk og dynamisk IP-adressering Konfigurere DHCP og NAT Arbeide med Cisco IOS Konfigurere VLAN-er Feilsøking i nettverk
Skyadministrasjon • Hypervisorer og virtuelle maskiner • Containere • Sikring av virtuelle miljøer • Sikkerhetskopiering og gjenopretting • Skyberegning og CSP-er • Hva er skytjenestemodeller • Typer av skyimplementering • Virtuelle nettverk • AWS-databehandlingstjenester • Amazon Elastic Compute Cloud (EC2) • Verktøy for skymonitorering • Verktøy for automatisering og koordinering • Sikkerhetstrusler og sårbarheter i skyen	4	0,5	2	0,5	**7**	**3,5**	Opprette virtuelle maskiner Konfigurere containere Sikring av virtuelle miljøer Arbeide med sikkerhetskopier Administrasjon av nettverk i skyen Konfigurere virtuelle nettverk Arbeide med verktøy for skymonitorering Implementering av automatisering og orkestrering Oppdage sikkerhetstrusler og sårbarheter i skyen

• Identitets- og tilgangsadministrasjon (IAM) • Rollebasert tilgangskontroll (RBAC) • Multifaktorautentisering (MFA) • Kryptering av skydata • Virtuell privat sky (VPC) • Docker og Kubernetes							Konfigurere identitets- og tilgangsadministrasjon (IAM) Implementering av skysikkerhetskrypterin g Arbeide med Docker og Kubernetes
Administrasjon av cyber-fysiske systemer • Sikkerhet og tilgangskontroll • Autentiseringstyper • TACACS+ og RADIUS • AAA-konfigurasjon • Risikostyringsmål • Kryptering og dekryptering • Hashing og regnbuetabeller • MAC-spoofing og ARP-forgiftning • VLAN-hopping og uautorisert DHCP • ICMP-flom • TCP- og UDP-flom • Sesjonskapring • DNS-spoofing • Defense in Depth (DID) og Zero Trust • Demilitariserte soner (DMZ) • Honeypots og nettverkssikring • Beste praksis for et sikkert nettverk • VPN • SSH og VNC • Stateful vs. stateless brannmurer • Vertbaserte vs. nettverksbaserte • Maskinvare- vs. programvare-brannmurer • Webapplikasjonsbrannmur (WAF) • AI i brannmurer • IDS og IPS • NIDS og HIDS • Snort • tcpdump	4	0,5	2	0,5	**7**	**3,5**	Innretning av infrastruktur Hovedkomponenter Implementering av sikkerhetskontroller Arbeide med TACACS+ og RADIUS AAA-konfigurasjon Lek med kryptering og dekryptering Analysere vanlige angrep og forsvarsteknikker Oppsett av demilitariserte soner (DMZ) Undersøkelse av honeypots Sikring gjennom beste praksis for et sikkert nettverk Installere VPN Arbeid med Secure Shell (SSH) Arbeide med Virtual Network Computing (VNC) Brannmurteknikker Implementering av AI i brannmurer Bruk av Snort og tcpdump for beskyttelse og deteksjon
Systemherding • GenAI-teknikker • Kodegenerering • Brukerkontoadministrasjon og tilgangskontroll • Deteksjon av avvik og feilsøking • Løse Apache2-tjenestefeil • Patchadministrasjon og oppdateringer	4	0,5	2	0,5	**7**	**3,5**	Arbeide med GenAI-teknikker Brukerkontoadministrasjon og tilgangskontroll Deteksjon av avvik og feilsøking Løse Apache2-tjenestefeil med GenAI Konfigurere patchadministrasjon og oppdateringer

• Automatisk sikkerhetskopiering og gjenoppretting • IT-ressursadministrasjon og inventar • Gjenoppretting av slettede filer med GenAI • Prosedyrer for cybersikkerhet • Trusseloppdagelse og analyse • Trueerespons og utbedring • Utnyttelse av AI for trusseloppdagelse i sanntid • Validering og testing av GenAI-modeller • Styring og regelverk • DNS-konfigurasjon og sikkerhet • DHCP-konfigurasjon og sikkerhet • Grunnleggende om PowerShell • Sikkerhet for switch-porter • Network Basic Input/Output System (NetBIOS) • Server Message Block Protocol (SMB) • Secure Sockets Layer (SSL) og Transport Layer Security (TLS) • Sikkerhetssertifikater • E-postsystemprotokoller • Domain Name System Protocol (DNS) • Filoverføringsprotokoll (FTP) • Fjernskrivebordsprotokoll (RDP) • Planlegging av oppgaver i Linux • Feilsøking av server • Feilsøking av nettverk • Sikkerhetskopiering og gjenopretting • Sikring av GRUB • Konfigurere og sikre brannmurer							Konfigurere automatisk sikkerhetskopiering og gjenoppretting Administrere IT-ressurser Gjenoppretting av slettede filer med GenAI Implementering av DNS- og DHCP-sikkerhet Arbeide med Microsoft BitLocker og Microsoft AppLocker Konfigurere Microsoft Firewall Konfigurere Switch Port Security Sikring av filoverføringsprotokoll (FTP) Sikring av Remote Desktop Protocol (RDP) Planlegge sikkerhetsoppgaver i Linux Sikring av GRUB Konfigurere og sikre brannmurer (iptables)
Tilgjengelighet • IR vs. SOC • Hendelser og incidenter • Deteksjon og prioritering av varsler • Dokumentasjon og rapportering • Hva er nettangrep? • DoS og DDoS • SQL-injeksjon og XSS • Kommandoinjeksjon og lokal fil-inkludering (LFI) • Cross-Site Request Forgery (CSRF) • Brute-Force og Credential Stuffing • Pass the Hash og Pass the Ticket • LDAP-rekognosering	4	0,5	3	0,5	**8**	4	Oppdage hendelser og incidenter Utføre varslingstriage Utarbeide dokumentasjon og korrekt rapportering Gjennomføring av aktiviteter etter hendelser Utføre og beskytte mot DoS og DDoS Oppdage nettangrep og spredning av skadelig programvare Utføre sikker statisk og dynamisk skadelig programvareanalyse Administrere IOC-er

• Brutt tilgangskontroll • Løsepenger • Datavirus og orm • Trojaner og adware • Keylogger og kryptojacking • Fileløs skadelig programvare • Forstå spredningen av skadelig programvare • Statisk og dynamisk analyse av skadelig programvare • Sikker analyse av skadelig programvare • Hybrid analyse Malware-etterforskning • Utføre statisk og dynamisk analyse av skadelig programvare • Administrere IOC-er og passordretningslinjer • Retningslinjer for akseptabel bruk (AUP) • Retningslinjer for bruk av egen enhet (BYOD) • Retningslinjer for ekstern tilgang							Opprette passordretningslinjer Konfigurere BYOD-retningslinjer (Bring Your Own Device) Opprette retningslinjer for ekstern tilgang
Totalt	**28**	**3,5**	**15**	**3,5**	**50**	**25**	

Vurderingsstrategi	**Sammenlignende vektprosent**	**Vurderingskriterier**
Selvbedømmelsestest (1)	5 %	10 poeng – 95–100 % riktige svar. 9 poeng – 85–94 % riktige svar. 8 poeng – 75–84 % riktige svar. 7 poeng – 65–74 % riktige svar. 6 poeng – 55–64 % riktige svar. 5 poeng – 45–54 % riktige svar. 4 poeng – 35–44 % riktige svar. 3 poeng – 25–34 % riktige svar. 2 poeng – 15–24 % riktige svar. 1 poeng – 0–14 % riktige svar.
Selvtest (2)	5 %	
Selvvalueringstest (3)	5 %	
Selvvalueringstest (4)	5	
Selvvalueringstest (5)	5	
Selvvalueringstest (6)	5 %	
Selvtest (7)	5	
Kunnskapsvurderingstest	65 %	

3. M3: ANALYTISKE VERKTØY

Modultittel	**Modulens kode**
ANALYTISKE VERKTØY	

Foreleser(e)	Institusjon eller avdeling hvor modulen undervises

Undervisningsform	Språk
Ansikt til ansikt, online, hybrid	*Engelsk, finsk, tyrkisk, norsk, litauisk, rumensk, fransk, polsk, spansk*

Forutsetninger
Ingen

Antall tildelte ECTS-poeng	Studentens arbeidsbelastning	Kontaktarbeidstimer	Individuelle arbeidstimer
3	75	5	25

Formål og resultater av modulen		
Etter å ha fullført dette kurset vil studentene ha tilegnet seg ferdigheter i å beskytte organisasjonens ressurser ved hjelp av ytelsesmålinger, dataanalyse og sikkerhetsinformasjon. De vil lære å bruke analyseverktøy effektivt for å identifisere potensielle cybersikkerhetsrisikoer og sårbarheter, utnytte datadrevne innsikter for å forbedre sikkerhetstiltak og bruke ytelsesmålinger relatert til passord, nettleserbruk, e-post og databehandlingsapplikasjoner. Ved slutten av modulen vil deltakerne være i stand til å evaluere og redusere potensielle sikkerhetstrusler ved hjelp av egnede verktøy og rapportere eventuelle trusler eller forstyrrelser til de riktige reguleringskanalene.		
Læringsutbytte av modulen	**Undervisnings- og læringsmetoder**	**Vurderingsmetoder**
Kunnskap: Deltakerne vil tilegne seg praktisk kunnskap om hvordan de kan bruke ytelsesmålinger, dataanalyse og sikkerhetsinformasjon til å beskytte organisasjonens ressurser.	Velges av foreleseren fra del 1.3. [Undervisningsmetoder, f.eks. teoretiske forelesninger, gjesteforelesere, spørrekonkurranser, spill, praktiske oppgaver/laboratorier, peer-to-peer-undervisning og -læring, selvstyrt læring osv.	Selvtest Kunnskapsvurderingstest
Ferdigheter: Elevene vil bli dyktige i å bruke analytiske verktøy for å identifisere potensielle cybersikkerhetsrisikoer og sårbarheter, anvende datadrevne innsikter for å styrke cybersikkerhetspraksis og utnytte ytelsesmålinger for å evaluere og forbedre sikkerheten til passord, nettlesing, e-post og datahåndtering.	Velges av foreleseren fra del 1.3. [Undervisningsmetoder, f.eks. praktiske oppgaver/laboratorier, praktiske aktiviteter, simulerte miljøer, spørrekonkurranser, spill, casestudier osv.] i D2.3 «Strukturen i læringsløpet for SMB-cybersikkerhetsagenter»	Praktiske vurderinger

Kompetanse: Lærerne vil være kompetente i å vurdere og redusere potensielle sikkerhetstrusler ved hjelp av analytiske verktøy, og nøyaktig rapportere trusler og brudd til de riktige kanalene i organisasjonen.	Velges av foreleseren, fra del 1.3. [Undervisningsmetoder, f.eks. simulerte miljøer, capture the flag-konkurranser, 5E, CBL, CL, POGIL, PBL osv.] i D2.3 «Strukturen i læringsløpet for SMB-cybersikkerhetsagenter»	Simuleringer Konkurranser

Modulens innhold: oversikt over emnene	**Kontaktarbeidstimer**					**Individuelle arbeidstimer og oppgaver**	
	Forelesninger (HEI)	Konsultasjoner	Praksis (HEI)	Tester	**Alt kontaktarbeid**	**Individuelt arbeid**	**Oppgaver**
Prestasjonsmålinger (målinger) • Ytelsesmetrikker • System- og nettverksovervåking • Overvåking av ytelsesmetrikker • Nettverkskartlegging • Sårbarhetsskanning • Analyse av nettverkstrafikk	10	0,5	5	0,5	**16**	**8,5**	• Gjennomfør forskning på ytelsesmålinger og verktøy. Sammenlign verktøy for ytelsesovervåking og identifiser forskjellene mellom dem. • Fullfør installasjonen av Zabbix og utfør grunnleggende konfigurasjon. • Lag en applikasjon for å overvåke ytelsesmålinger med Zabbix. • Identifiser sårbarheter i målsystemet ved hjelp av nettverkskartleggingsprogramvare (for eksempel nmap, rustscan osv.). • Utfør en sårbarhetsskanning på målsystemet ved hjelp av Nessus-programvare. Utarbeid en rapport om sårbarhetstesting. • Utfør nettverkstrafikanalyse ved hjelp av Wireshark.
Dataanalyse • Datainnsamling • Datarengjøring og forbehandling • Dataanalyse	10	0,5	5	0,5	**16**	**8,5**	• Utfør datarengjøring og forbehandling av et datasett relatert til cybersikkerhetsproblemer

• Datavisualisering • Analytiske verktøy • Anvendelser av dataanalyse i cybersikkerhet							utarbeidet for en hypotetisk SMB. • Analyser det rensede og forbehandlede datasettet fra den hypotetiske SME-bedriften og visualiser resultatene. • Hva er eksempler på dataanalyseapplikasjoner innen cybersikkerhet? Vennligst undersøk.
Sikkerhetsinformasjon • Forstå sikkerhetsinformasjon • Kilder til sikkerhetsinformasjon • Metoder for innsamling av trusselinformasjon • Rammer for trusselinformasjon • AI-drevne sikkerhetsinformasjonsplattformer • Casestudier om sikkerhetsinformasjonsapplikasjoner	10	0,5	7	0,5	**18**	**8**	• Undersøk hvordan sikkerhetsinformasjon bidrar til SMB-bedrifters proaktive sikkerhetsstrategier. • Hva er de vanligste kildene for å innhente sikkerhetsinformasjon? Hvordan vurderer du påliteligheten til disse kildene? • Definer fordelene og begrensningene ved hver metode for innsamling av trusselinformasjon. • Forklar kjernefunksjonene i rammeverk for trusselinformasjon, som MITRE ATT&CK og Cyber Kill Chain. • Undersøk en reell casestudie der sikkerhetsinformasjon ble brukt. Beskriv metodene for innsamling av informasjon som ble brukt i den casestudien.
Totalt	**30**	**1,5**	**17**	**1,5**	**50**	**25**	

Vurderingsstrategi	Sammenlignende vektprosent	Vurderingskriterier
Selvtest I	15	10 poeng – 95–100 % riktige svar. 9 poeng – 85–94 % riktige svar. 8 poeng – 75–84 % riktige svar. 7 poeng – 65–74 % riktige svar. 6 poeng – 55–64 % riktige svar. 5 poeng – 45–54 % riktige svar. 4 poeng – 35–44 % riktige svar. 3 poeng – 25–34 % riktige svar. 2 poeng – 15–24 % riktige svar. 1 poeng – 0–14 % riktige svar.
Selvtest II	15	
Selvtest III	15	
Kunnskapsvurderingstest	55	

Studiemateriale *(Etternavn, forbokstav. (År, måned, dag). Artikkelens tittel. Tidsskrift/journal/avisens tittel, volumnummer (utgavenummer), sidetall for hele artikkelen, utgiver, URL)*
Obligatorisk lesning
…
Anbefalt lesning
https://brainstation.io/career-guides/what-tools-do-cybersecurity-analysts-use **https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it** **https://medium.com/@jcm3/wireshark-traffic-analysis-part-1-tryhackme-walkthrough-a9bec11d94d9** **https://www.kali.org/tools/nmap/** **https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/** **https://www.varonis.com/blog/cyber-kill-chain** **https://www.youtube.com/watch?v=kVnvIBNiC58**

4. M4: SIKKERHETSOPERASJONER

Modultittel	Modulnummer
SIKKERHETSOPERASJONER	

Foreleser(e)	Institusjon eller avdeling hvor modulen undervises

Undervisningsform	Språk
Ansikt til ansikt, online, blandet, konsultasjoner	*Engelsk, finsk, tyrkisk, norsk, litauisk, rumensk, fransk, polsk, spansk*

Forutsetninger
Ingen

Antall tildelte ECTS-poeng	Studentens arbeidsbelastning	Kontaktarbeidstimer	Individuelle arbeidstimer
3	75	50	25

Formål og læringsutbytte		
Etter å ha fullført dette kurset vil studentene være i stand til å effektivt administrere sikkerhetsoperasjoner innenfor IKT-infrastrukturer, -systemer og -tjenester. De vil tilegne seg ferdigheter i å overvåke, oppdage, reagere på og gjenopprette etter cybersikkerhetshendelser ved å anvende beste praksis, verktøy og rammeverk som er relevante for sikkerhetsoperasjoner.		
Læringsutbytte av modulen	**Undervisnings- og læringsmetoder**	**Vurderingsmetoder**
Kunnskap: Studentene vil tilegne seg avansert kunnskap om sikkerhetsoperasjoner, inkludert overvåking, oppdagelse, hendelsesrespons og gjenoppretting. De vil være i stand til å etablere og beskrive effektive operasjonelle rutiner for cybersikkerhet som er tilpasset de spesifikke behovene til SMB-arbeidsplasser i samsvar med cybersikkerhetsstandarder.	Velges av foreleseren fra del 1.3. [Undervisningsmetoder, f.eks. teoretiske forelesninger, litteraturanalyse, gjesteforelesere, peer-to-peer-undervisning og -læring, veiledning osv.	Selvtest Kunnskapsvurderingstest

Ferdigheter: Deltakerne vil være dyktige i å anvende avanserte metoder og verktøy for å utføre sikkerhetsoperasjoner, utforme og implementere effektive overvåkingsstrategier, håndtere sikkerhetshendelser og utvikle robuste operasjonelle rutiner spesielt tilpasset SMB-arbeidsplasser.	Velges av foreleseren fra del 1.3. [*Undervisningsmetoder, f.eks. teoretiske forelesninger, litteraturanalyse, gjesteforelesere, peer-to-peer-undervisning og læring, veiledning osv.]* av D2.3 «*Strukturen i læringsløpet for SMB-cybersikkerhetsagenter*»	Selvtest Kunnskapsvurderingstest
Kompetanse: Lærerne vil være kompetente i å utvikle og implementere strategiske sikkerhetsoperasjonspolitikker og -prosedyrer for SMB-arbeidsplasser.	Velges av foreleseren fra del 1.3. [*Undervisningsmetoder, f.eks. teoretiske forelesninger, litteraturanalyse, gjesteforelesere, peer-to-peer-undervisning og læring, veiledning osv.]* i D2.3 «*SME Cyber Security Change Agents Learning Pathway's* Structure» (Strukturen i læringsløpet for endringsagenter innen cybersikkerhet i SMB).	Selvvalueringstester Kunnskapsvurderingstest

Modulens innhold: oversikt over emnene	**Kontaktarbeidstimer**					**Individuelle arbeidstimer og oppgaver**	
	Forelesninger	Konsultasjoner	Praksis (HEI)	Tester	Alt	Individuelt arbeid	Oppgaver

Grunnleggende sikkerhetsoperasjoner - Forstå sikkerhetsoperasjoner og SOC (Security Operations Centre) - Roller og ansvar i sikkerhetsoperasjoner - Oversikt over verktøy og teknologier for sikkerhetsoperasjoner	6	0,5	2	0,5	**9**	6	Identifisere og forstå strukturen og funksjonen til et SOC, analysere ulike roller innen sikkerhetsoperasjoner, undersøke verktøy som brukes i sikkerhetsoperasjoner og analysere en casestudie.
Sikkerhetskonvergens - Forstå sikkerhetskonvergens - Grunnleggende om fysisk sikkerhet (prinsipper for fysisk sikkerhet, beskyttelse av fysiske eiendeler, retningslinjer) - Case-studie som belyser prinsippene for sikkerhetskonvergens	8	0,5	4	0,5	**13**	6	Gjennomgå definisjonen og prinsippene for sikkerhetskonvergens, erkjenn viktigheten av å integrere fysiske og digitale sikkerhetsoperasjoner, identifiser og vurder risikoer på tvers av cyber- og fysiske domener.
Sikkerhetsinformasjon og hendelsesstyring - Gjennomgang av prinsipper for sikkerhetsovervåking - Implementering av SIEM-løsninger	8	0,5	4	0,5	**13**	6	Introduksjon til sikkerhetsovervåking og SIEM-implementering. Grunnleggende prinsipper som loggtyper, deteksjonsmetoder og overvåkingssyklus. Praktiske aspekter ved implementering av SIEM, inkludert arkitektur, datainnsamling, regeloppretting og varslingshåndtering.

Sikkerhetsoperasjonspraksis - Identifisere datakilder og optimalisere logginnsamling - Sentralisere varsler med SIEM - Testing av SIEM	4	0,5	10	0,5	**15**	7	Omfattende og praksisorientert opplæringsprogram med grunnleggende kunnskap og praktiske ferdigheter innen loggadministrasjon, SIEM-konfigurasjon og trusseloppdagelse i ulike IT-miljøer.
Totalt	**26**	**2**	**20**	**2**	**50**	**25**	

Vurderingsstrategi	**Sammenlignende vektprosent**	**Vurderingskriterier**
Selvbedømmelsestest (1)	10 %	10 poeng – 95–100 % riktige svar. 9 poeng – 85–94 % riktige svar. 8 poeng – 75–84 % riktige svar. 7 poeng – 65–74 % riktige svar. 6 poeng – 55–64 % riktige svar. 5 poeng – 45–54 % riktige svar. 4 poeng – 35–44 % riktige svar. 3 poeng – 25–34 % riktige svar. 2 poeng – 15–24 % riktige svar. 1 poeng – 0–14 % riktige svar.
Selvtest (2)	10 %	
Selvvalueringstest (3)	10 %	
Selvvalueringstest (4)	10	
Kunnskapsvurderingstest	60 %	

Studiemateriale *(Etternavn, forbokstav. (År, måned, dag). Artikkelens tittel. Tidsskrift/journal/avisens tittel, volumnummer (utgavenummer), sidetall for hele artikkelen, utgiver, URL)*
Obligatorisk lesning
Cybellium (2024). *Studieveiledning til sikkerhetsoperasjonssentre (SOC): En omfattende veiledning for å lære om sikkerhetsoperasjonssentre (SOC)* Muniz, J. (2021). *Det moderne sikkerhetsoperasjonssenteret*. Pearson Education. ENISA (2017). *Strategier for håndtering av hendelser og samarbeid om cybersikkerhet*. **Strategier for håndtering av hendelser og samarbeid om cybersikkerhet — ENISA (europa.eu)**
Anbefalt lesning
Basta, A., Basta, N., Anwar, W., Essar, M. I. (2024). Åpent sikkerhetsoperasjonssenter (SOC): En komplett guide til etablering, administrasjon og vedlikehold av et moderne SOC. Cybellium (2023). Administrere et sikkerhetssenter (SOC).

5. M5: SIKKERHETSSTYRING OG -POLICYER

Modultittel	Modulkode
SIKKERHETSTYING OG POLICYER	

Foreleser(e)	Institusjon eller avdeling hvor modulen undervises

Undervisningsform	Språk
Ansikt til ansikt / Online / Hybrid	*Engelsk, finsk, tyrkisk, norsk, litauisk, rumensk, fransk, polsk, spansk*

Forutsetninger
Ingen

Antall tildelte ECTS-poeng	Studentens arbeidsbelastning	Kontaktarbeidstimer	Individuelle arbeidstimer
3	75	5	25

Formål og resultater av modulen
Faget «Sikkerhetsstyring og -policyer» har som mål å forberede studentene på å møte utfordringene knyttet til cybersikkerhet i små og mellomstore bedrifter, integrere sikkerhetsstyring i forretningsstrategien og sikre overholdelse av lovbestemmelser, som for eksempel GDPR. Modulen dekker aspekter som identifisering av trusler og sårbarheter, utforming av robuste og adaptive sikkerhetsretningslinjer og effektiv håndtering av hendelser. I tillegg fokuserer den på å utvikle styringsstrukturer som tildeler klare roller i organisasjonen, og som samordner cybersikkerhet med strategiske mål. Studentene vil tilegne seg tekniske kompetanser innen risikovurdering og risikoreduksjon på nettet, og utvikle analyseferdigheter for å foreslå forbedringer i sikkerhetsmodenhet. De vil også bli dyktige i å kommunisere cybersikkerhetsbehov effektivt til ledere, støtte informerte beslutninger og sikre overholdelse av regelverk og etikk innen cybersikkerhet. Modulen «Sikkerhetsstyring og -policyer» inneholder også en fokusert gjennomgang av forebygging av phishing, AI-drevne cyberangrep og håndtering av ransomware, og analyserer hvordan disse spesifikke truslene krever en integrert tilnærming til styring og etterlevelse. Effektiviteten av sikkerhetspolicyer vil ikke bare måles ut fra deres evne til å forhindre hendelser, men også ut fra deres tilpasningsevne til nye trusler og etterlevelse av gjeldende lovbestemmelser.

Læringsutbytte av modulen	Undervisnings- og læringsmetoder	Vurderingsmetoder
Kunnskap: Deltakerne vil få avansert kunnskap om hvordan man implementerer nye rutiner og arbeidsflyter for cybersikkerhet på arbeidsplasser i små og mellomstore bedrifter, ved å innlemme gjeldende prinsipper for cybersikkerhet, trender og overholdelse av nasjonal og internasjonal lovgivning som er relevant for deres bransje. Få avansert kunnskap om hvordan man integrerer forebygging av phishing, håndterer AI-drevne trusler og responderer på ransomware i SMB-miljøer	**Forelesninger (veiledet lesing):** Forelesningene gir et solid konseptuelt grunnlag i cybersikkerhet, styring, personvern og samsvar, og oppmuntrer til aktiv deltakelse fra studentene. Inkluderer interaktive forelesninger som inneholder regelmessige spørsmål og svar-sesjoner, avstemninger og live problemløsningsøvelser. Ved hjelp av verktøy som Mentimeter og Poll Everywhere, **Deltakelse i diskusjoner og fora:** Deltakelse i diskusjoner og fora vil gi studentene mulighet til å debattere og kritisk analysere cybersikkerhetsspørsmål, og dermed utvikle sine argumentasjonsevner. Dette vil bli brukt på spørsmål knyttet til etikk, retningslinjer og beslutningstaking innen cybersikkerhet. **Casestudier:** Casestudiene vil gi studentene mulighet til å analysere cybersikkerhetssituasjoner i små og mellomstore bedrifter, og anvende teoretisk kunnskap for å løse reelle problemer. De vil fokusere på temaer som håndtering av datainnbrudd, ransomware, phishing, AI-drevne angrep, implementering av sikkerhetspolitikk og styring.	**Selvtest:** Selvtestene gir studentene mulighet til å vurdere sin forståelse av hvert delemne gjennom en rekke spørsmål, og gir kontinuerlig tilbakemelding for å identifisere områder som kan forbedres. De påvirker ikke den endelige karakteren, men er viktige for selvstyrt læring. **Avsluttende eksamen (valgfritt):** Avsluttende eksamen er valgfri og gir studentene mulighet til å oppnå et fullføringsbevis ved å evaluere sin samlede forståelse av kurset gjennom utviklingsspørsmål, case-analyse og flervalgsspørsmål. Det er nødvendig å bestå eksamen for å oppnå fullføringsbeviset, mens de som ikke tar eksamen, vil motta et deltakerbevis.
Ferdigheter: Deltakerne vil bli dyktige i å bruke avanserte metoder for å gjennomføre risikovurderinger, utforme og implementere nye rutiner for cybersikkerhet og utarbeide responsstrategier, slik at effektiv styring og etterlevelse sikres på arbeidsplasser i små og mellomstore bedrifter.	**Praktiske workshops:** De praktiske workshopene vil gi studentene mulighet til å anvende cybersikkerhetskonsepter gjennom øvelser som policyutvikling og simuleringer av hendelser, med tilbakemeldinger i sanntid fra instruktøren. De er utformet for å styrke praktiske ferdigheter og forberede studentene på å anvende det de har lært i reelle situasjoner.	**Praktiske vurderinger:** Praktiske vurderinger gjennom hele kurset vil gi studentene mulighet til å anvende teoretisk kunnskap i simulerte situasjoner, for eksempel utvikling av cybersikkerhetsretningslinjer og simuleringer av hendelser, med det formål

Utvikle ferdigheter i å utforme og implementere omfattende rutiner for cybersikkerhet som håndterer avanserte trusler og sikrer organisasjonens samsvar.	**Praktisk arbeid og individuelle prosjekter:** Praktisk arbeid og individuelle prosjekter vil gi studentene mulighet til å anvende cybersikkerhetskonsepter gjennom oppgaver som utarbeidelse av retningslinjer og risikoanalyse, utvikling av autonome arbeidsferdigheter og praktisk anvendelse av teoretisk kunnskap. **Samarbeidsprosjekter:** Samarbeidsprosjekter vil gi studentene mulighet til å jobbe i team for å utvikle cybersikkerhetsløsninger for SMB-bedrifter, inkludert sikkerhetsretningslinjer og styringsmodeller. De vil fremme teamarbeid, prosjektledelse og praktisk anvendelse av tilegnet kunnskap, med tilbakemeldinger fra lærere og medstudenter.	å vurdere deres evne til å løse reelle problemer i SMB-sammenheng. **Gruppeprosjekter:** Gruppeprosjekter vil gi studentene mulighet til å utvikle et omfattende cybersikkerhetsprosjekt, fra risikoidentifisering til forslag til styringsmodeller og beredskapsplaner, og evaluere både kvaliteten på innholdet og evnen til å samarbeide. Dette prosjektet er avgjørende for den endelige vurderingen og integrerer all læring i kurset.
Kompetanse: Studentene vil være kompetente i å utvikle og implementere strategiske cybersikkerhetspolitikker, lede initiativer for å etablere nye rutiner og arbeidsflyter på SMB-arbeidsplasser, og ta etiske beslutninger som er i tråd med organisasjonens mål og krav til samsvar. Bli kompetent i å formulere og gjennomføre retningslinjer for cybersikkerhet som forhindrer sofistikerte cybertrusler og sikrer samsvar med internasjonale cybersikkerhetsforskrifter.	**Scenariosimuleringer:** Scenariosimuleringer vil gjøre det mulig for studentene å håndtere cybersikkerhetshendelser i virtuelle miljøer som replikerer reelle angrep, og ta strategiske beslutninger under press. Denne metoden forbedrer ferdighetene i krisehåndtering og hendelsesrespons, og er avgjørende for å undervise i evaluering av sikkerhetspolitikk og beslutningstaking i kritiske situasjoner. Studentene må demonstrere hvordan de vil anvende styringsretningslinjer for å forhindre eller respondere på spesifikke hendelser som phishing-angrep, ransomware og AI-drevne angrep, og vurdere deres forståelse av det relevante regelverket.	**Simuleringer og hendelseshåndtering:** Studentene vil bli vurdert på deres evne til å håndtere cybersikkerhetshendelser i simuleringer som gjenskaper reelle kriser i en SMB. Målet er å måle deres evne til å håndtere press, ta strategiske beslutninger og gjennomføre responsplaner i sanntid, og vurdere deres praktiske anvendelse i dynamiske situasjoner.

Modulens innhold: oversikt over emnene	Kontaktarbeidstimer					Individuelle arbeidstimer og oppgaver	
	Forelesninger	Konsultasjoner	Praksis (HEI)	Tester	**Alt**	**Individuelt**	**Oppgaver**
Organisatorisk kontekst -Utviklingen av cybersikkerhet i små og mellomstore bedrifter -Aktuelle store trusler og sårbarheter -Cybersikkerhetens innvirkning på forretningsstrategien -Spesifikke utfordringer knyttet til cybersikkerhet i SMB-bedrifter sammenlignet med store bedrifter - Forstå de regulatoriske implikasjonene av cybersikkerhetspraksis og hvordan de samsvarer med styringsstrukturer. - Vanlige utfordringer knyttet til cybersikkerhet som er spesifikke for SMB-bedrifter, for eksempel begrensede budsjetter, mangel på dedikert sikkerhetspersonell og praktiske metoder for å prioritere investeringer i cybersikkerhet.	5	0,5	3	0,5	**9**	**4**	Lesing, forskning, forberedelse av casestudier
Personvern -Personvernprinsipper i cybersikkerhet -Beskyttelse av personopplysninger og GDPR -Personvernets innvirkning på SMB-virksomhet -Verktøy og teknikker for personvern	4	0,5	3	0,5	**8**	**4**	Politikanalyse, individuell oppgave
Lover, etikk og samsvar -Cybersikkerhet Organisasjoner, politikk og standarder -Relevant nasjonal og internasjonal lovgivning -Regulatorisk compliance i SMB-bedrifter -Etikk i cybersikkerhet -Juridiske konsekvenser av manglende etterlevelse innen cybersikkerhet - Analyse av hvordan AI-baserte verktøy kan brukes til å styrke cybersikkerhetsstyringen og sikre overholdelse gjennom kontinuerlig overvåking og automatisert trusselrespons.	5	0,5	3	0,5	**9**	**5**	Casestudie, lovgivningsanalyse

Sikkerhetsstyring -Styringsstruktur for cybersikkerhet -Roller og ansvar i sikkerhetsstyring -Modeller for modenhet innen cybersikkerhet -Integrering av cybersikkerhet i selskapsstyring - Forbedre evnen til å gjennomføre risikovurderinger og utarbeide strategiske beredskapsplaner under simulerte krisesituasjoner (ransomware, phishing-angrep, ...)	4	0,5	3	0,5	**8**	**4**	Risikostyringsscenarioanalyse
Kommunikasjon på ledelses- og styrenivå -Kommunikasjonsstrategier for cybersikkerhet -Sikkerhetsrapportering til toppledelsen -Beslutningstaking basert på sikkerhetsdata -Kriseledelse og kommunikasjon innen cybersikkerhet -Mestre krisehåndtering og beslutningstaking i stressende situasjoner som involverer AI-drevne angrep og løsepengevirus.	4	0,5	3	0,5	**8**	**4**	Presentasjonsforberedelse, kommunikasjon med interessenter
Ledelsespolitikk -Utvikling av sikkerhetspolitikk -Implementering og overvåking av policy -Evaluering og kontinuerlig forbedring av politikk -Tilpasning av sikkerhetspolitikk til teknologiske og regulatoriske endringer - Utforsking av hvordan effektive opplærings- og bevisstgjøringspolitikker kan være en avgjørende komponent i regelverksetterlevelse og risikoreduksjon.	4	0,5	3	0,5	**8**	**4**	Skriving og revisjon av et policydokument
Totalt	**26**	**3**	**18**	**3**	**50**	**25**	

Vurderingsstrategi	**Sammenlignende vektprosent**	**Vurderingskriterier**
Selvtest I	10	Vurdering av grunnleggende begreper om organisatorisk kontekst.
Selvtest II	10	Vurdering av grunnleggende begreper om personvern.
Selvtest III	10	Evaluering av lover, etikk og retningslinjer for samsvar.
Selvtest IV	10	Evaluering av retningslinjer for cybersikkerhet.
Selvtest V	10	Vurdering av kommunikasjon på ledernivå.
Selvtest VI	10	Evaluering av ledelsespolitikk og utforming av sikkerhetspolitikk.
Kunnskapsevalueringstest	40	Avsluttende eksamen som dekker integrerende spørsmål om alle emner i kurset.
10 poeng – 95–100 % riktige svar. 9 poeng – 85–94 % riktige svar.		

8 poeng – 75–84 % riktige svar.
7 poeng – 65–74 % riktige svar.
6 poeng – 55–64 % riktige svar.
5 poeng – 45–54 % riktige svar.
4 poeng – 35–44 % riktige svar.
3 poeng – 25–34 % riktige svar.
2 poeng – 15–24 % riktige svar.
1 poeng – 0–14 % riktige svar.

Studiemateriale *(Etternavn, første initial. (År, måned, dag). Artikkelens tittel. Magasin/tidsskrift/avisens tittel, volumnummer (utgavenummer), sidetall for hele artikkelen, utgiver, URL)*

Obligatorisk lesning

...

«EU Cybersecurity Law: Governing Resilience and Coherence in the Digital Age» av Luisa Marin

- Denne boken gir en grundig analyse av EUs lover og politikk for cybersikkerhet, noe som er avgjørende for å forstå hvordan cybersikkerhetsstyring er strukturert og implementert i EU-sammenheng.

«Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy» av George Christou

- Denne boken utforsker styringsrammer og beslutningsprosesser for cybersikkerhet i EU, og hjelper studenter å forstå det dynamiske samspillet mellom ulike styringsnivåer.

«Phishing og mottiltak: Forståelse av det økende problemet med elektronisk identitetstyveri» av Markus Jakobsson og Steven Myers

- Selv om denne boken ikke er spesifikk for EU, kan den detaljerte utforskningen av phishing-teknikker og mottiltak kontekstualiseres innenfor EU ved å fokusere på GDPR-samsvar og prinsipper for databeskyttelse.

«European Cybersecurity Law and Regulation» redigert av Nadya Purtova og Bert-Jaap Koops

- Denne redigerte utgaven dekker juridiske og regulatoriske tiltak som er spesifikke for cybersikkerhet i Den europeiske union, inkludert utfordringer knyttet til samsvar og rammeverk som NIS-direktivet og GDPR.

«Ransomware: Understanding Digital Extortion and its Threat to Your Organization» av Allan Liska og Timothy Gallo

- Denne teksten, supplert med EU-spesifikke casestudier og eksempler, vil hjelpe studentene å forstå implikasjonene av ransomware-angrep under EU-regelverket.

Anbefalt lesning

«EU-forordningen om personvern (GDPR): En kommentar» av Lukas Feiler og Nikolaus Forgó

- Denne kommentaren gir detaljert innsikt i GDPR, som er viktig for å forstå regelverket i EU og dets innvirkning på cybersikkerhetspraksis.

«Databeskyttelse og cybersikkerhet i Europa: Juridiske rammeverk og praktiske hensyn» av Paul Lambert

- Denne boken gir praktisk innsikt i samordningen av strategier for databeskyttelse og cybersikkerhet i EU, inkludert overholdelse av regelverk og beste praksis for sikkerhetstiltak.

«Network and Information Security: European and International Perspectives» redigert av Jeanne Pia Mifsud Bonnici og Joe Cannataci

- Denne samlingen undersøker nettverks- og informasjonssikkerhetslandskapet fra både europeiske og internasjonale perspektiver, og gir en bredere kontekst for EUs cybersikkerhetsarbeid.

«Kunstig intelligens i cybersikkerhet: praksis, utfordringer og etikk» av Elena Fersman og Martin Fredriksson

- En omfattende oversikt over integreringen av AI-teknologier i cybersikkerhet, som tar for seg etiske, operasjonelle og regulatoriske utfordringer, spesielt relevante i EU-sammenheng.

«Cybersecurity in the Digital Age: Tools, Techniques, and Applications» av Gregory B. White, Eric A. Fisher og James L. Antonakos

- Selv om denne boken ikke utelukkende fokuserer på EU, dekker den også et bredt spekter av moderne cybersikkerhet.

Studiemateriale *(HackerU og Cybints originale materiale)*
Obligatorisk lesning
• TCP/IP Network Administration: Help for Unix System Administrators 3. utgave, av Craig Hunt (O'Reilly) • Essential System Administration Pocket Reference: Kommandoer og filformater (Pocket Administrator) av Eleen Frisch (O'Reilly) • Datakommunikasjon: Begynnerveiledning for å mestre datakommunikasjon, Internett og OSI-modellen av Ramon Nastase
Anbefalt lesning
• CompTIA A+ Certification All-in-One For Dummies (Computer/Tech) 5. utgave av Glen E. Clarke, Edward Tetz, Timothy L. Warner • Coding All-in-One For Dummies 1. utgave av Nikhil Abraham • Grunnleggende informasjonsteknologi, bind 1: Introduksjon til informasjonssystemer av Eric Frick • IT-arkitektur for dummies, 1. utgave av Kalani Kirk Hausman, Susan L. Cook • Cybersecurity For Dummies (Datamaskiner/Teknologi) 1. utgave av Steinberg • Linux For Dummies, 10. utgave 10. utgave av Richard Blum • Windows 10 for dummies, 3. utgave (datamaskiner/teknologi) 3. utgave av Rathbone • Nettverk for dummies, 12. utgave av Doug Lowe

6. M6: PLANLEGGING AV CYBERSIKKERHET

Modultittel	Modulens kode
CYBERSIKKERHETSPLANLEGGING	

Foreleser(e)	Institusjon eller avdeling hvor modulen undervises

Undervisningsform	Språk
Ansikt til ansikt, online, blandet, konsultasjoner	*Engelsk, finsk, tyrkisk, norsk, litauisk, rumensk, fransk, polsk, spansk*

Forutsetninger
-

Antall tildelte ECTS-poeng	Studentens arbeidsbelastning	Kontaktarbeidstimer	Individuelle arbeidstimer
3	75	5	25

Formål og resultater av modulen

Etter å ha fullført dette kurset vil studentene være i stand til å forstå og anvende kjerneprinsippene for planlegging og styring av cybersikkerhet. De vil tilegne seg evnen til å implementere internasjonale standarder og rammeverk, utvikle langsiktige sikkerhetsstrategier, styre operasjonelle og taktiske cybersikkerhetstiltak og planlegge sikre nettverksarkitekturer som sky og nulltillit. Videre vil studentene være rustet til å utforme effektive beredskapsplaner og implementere strategier for forretningskontinuitet, som sikrer organisasjonens robusthet og effektive cybersikkerhetstiltak i møte med stadig nye trusler.

Læringsutbytte av modulen	Undervisnings- og læringsmetoder	Vurderingsmetoder
Kunnskap: Studentene vil tilegne seg avansert kunnskap om hvordan man integrerer avanserte prinsipper for cybersikkerhet og aktuelle trender i strategisk planlegging og operativ ledelse.	Forelesninger, casestudier, gruppediskusjoner, selvstyrt læring	Selvtest, kunnskapstester
Ferdigheter: Deltakerne vil tilegne seg ferdigheter i strategisk planlegging og operativ ledelse, slik at de effektivt kan utforme og implementere cybersikkerhetsstrategier som håndterer nye risikoer og sikrer robuste taktiske responser	Praktiske øvelser, workshops, casestudier	Prosjektbaserte vurderinger, praktiske evalueringer

Kompetanse: Deltakerne vil bli kompetente i å utvikle og implementere strategiske rammeverk for cybersikkerhet, samt lede og administrere cybersikkerhetstiltak	Workshops, seminarer, rollespilløvelser	Kontinuerlig vurdering, scenariebaserte tester

Modulens innhold: oversikt over emnene	**Kontaktarbeidstimer**					**Individuelle arbeidstimer og oppgaver**	
	Forelesninger	Konsultasjoner	Praksis (HEI)	Tester	**Alt kontaktarbeid**	**Individuelt arbeid**	**Oppgaver**
1. Introduksjon til cybersikkerhetsplanlegging: Data-, menneskelig og samfunnsmessig sikkerhet - datasikkerhet - sikkerhet ved lagring av informasjon, etterforskningsprosess - datasikkerhet – teknikker for passordangrep - menneskelig sikkerhet – bevissthet og forståelse - Samfunnssikkerhet – hva er nettkriminalitet, nettetikk - Samfunnssikkerhet – cyberlovgivning – digitale bevis, digitale kontrakter, multinasjonale konvensjoner (avtaler)	8	0,5	6	0,5	**15**	**8**	Definere de juridiske aspektene ved data, menneskelig og samfunnsmessig sikkerhet, lover og retningslinjer som regulerer data i SMB-er. Klassifiser typer cyberangrep som er relevante for SMB-er Identifisere nyttige verktøy for å forhindre cyberangrep
2. Strategisk planlegging -Definere mål og målsettinger for cybersikkerhet -SWOT-analyse (styrker, svakheter, muligheter, trusler) -Utvikle langsiktige sikkerhetsstrategier -Fastsette nøkkelindikatorer (KPI-er) -Gjennomgang og oppdatering av sikkerhetsstrategien	8	2	6	2	**18**	**8**	Definer cybersikkerhetsmål som er relevante for SMB-er ved hjelp av en SWOT-analyse, utvikle langsiktige strategier for å håndtere risiko, tildele ressurser og budsjett deretter, sett KPI-er for å måle fremgang, og oppdater strategien regelmessig basert på nye trusler.

3. Operativ og taktisk ledelse -Implementering av tilgangskontroll -Patchadministrasjon og programvareoppdateringer -Kontinuerlig systemovervåking - Opplæring av ansatte i sikkerhetsbevissthet	8	1	6	2	**17**	**9**	Implementer tiltak for tilgangskontroll for å begrense uautorisert tilgang, vedlikehold systemene gjennom patch-administrasjon, sett opp overvåking av uvanlige aktiviteter og gi ansatte opplæring i cybersikkerhet.
Totalt	**24**	**3,5**	**18**	**4,5**	**50**	**25**	

Vurderingsstrategi	**Sammenlignende vektprosent**	**Vurderingskriterier**
Selvtest (1)	10	10 poeng – 96–100 % riktige svar. 9 poeng – 91–95 % riktige svar. 8 poeng – 86–90 % riktige svar. 7 poeng – 80–85 % riktige svar. 6 poeng – 70–79 % riktige svar. 5 poeng – 60–69 % riktige svar. 4 poeng – 50–59 % riktige svar. 3 poeng – 40–49 % riktige svar. 2 poeng – 30–39 % riktige svar. 1 poeng – 0–29 % riktige svar.
Selvtest (2)	10	
Selvvalueringstest (3)	10	
Kunnskapsvurderingstest	70	

Studiemateriale *(Etternavn, forbokstav. (År, måned, dag). Artikkelens tittel. Tidsskrift/journal/avisens tittel, volumnummer (utgavenummer), sidetall for hele artikkelen, utgiver, URL)*

Obligatorisk lesning

1. Nair, A., & Greeshma, M. R. (2023). Mastering Information Security Compliance Management: A Comprehensive Handbook on ISO/IEC 27001:2022 Compliance. Packt Publishing Limited.
2. Falco, G. J., & Rosenbach, E. (2021). Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity. Oxford University Press.
3. NIST Cybersecurity Framework (CSF) 2.0, National Institute of Standards and Technology, 26. februar 2024

Anbefalt lesning

1. Mehta, S. (2023). *ISACA Certified in Risk and Information Systems Control (CRISC®) Exam Guide*. Packt Publishing Limited.
2. Gregory, P. H. (2021). *CISM-sertifisert informasjonssikkerhetsleder All-in-One eksamensguide*. McGraw-Hill.
3. ISACA. (2021). *CRISC Review Manual, 7. utgave*. ISACA.
4. Europaparlamentet og Rådet. (14. desember 2022). *Forordning (EU) 2022/2554 om digital operasjonell robusthet for finanssektoren*.
5. Guide to the General Data Protection Regulation (GDPR), Information Commissioner's Office

7. M7: RISIKOSTYRING OG RISIKOREDUKSJON

Modultittel	Modulens kode
RISIKOSTYRING OG RISIKOREDUKSJON	

Foreleser(e)	Institusjon eller avdeling hvor modulen undervises

Undervisningsform	Språk
Ansikt til ansikt, online, blandet, konsultasjoner	*Engelsk, finsk, tyrkisk, norsk, litauisk, rumensk, fransk, polsk, spansk*

Forutsetninger			
Ingen			
Antall tildelte ECTS-poeng	**Studentens arbeidsbelastning**	**Kontaktarbeidstimer**	**Individuelt arbeid**
3	75	5	25

Formål og læringsutbytte		
Etter å ha fullført dette kurset vil studentene være i stand til å kontinuerlig håndtere (identifisere, analysere, vurdere, estimere, redusere) cybersikkerhetsrelaterte risikoer ved IKT-infrastrukturer, -systemer og -tjenester ved å planlegge, anvende, rapportere og kommunisere risikoanalyse, -vurdering og -behandling.		
Læringsutbytte av modulen	**Undervisnings- og læringsmetoder**	**Vurderingsmetoder**
Kunnskap: Studentene vil tilegne seg avansert kunnskap om risikostyringsprosesser, inkludert risikoidentifisering, -vurdering og -kontroll, slik at de kan etablere og beskrive effektive cybersikkerhetsrutiner tilpasset de spesifikke behovene til SMB-arbeidsplasser i samsvar med nasjonale og internasjonale standarder.	Velges av foreleseren fra del 1.3. [*Undervisningsmetoder, f.eks. teoretiske forelesninger, litteraturanalyse, gjesteforelesere, peer-to-peer-undervisning og -læring, veiledning osv.*	Selvtest Kunnskapsvurderingstest
Ferdigheter: Lærerne vil være i stand til å anvende avanserte metoder og verktøy for å gjennomføre omfattende risikovurderinger, utforme og implementere effektive risikostyringsstrategier og utvikle robuste rutiner for cybersikkerhet som er spesielt tilpasset arbeidsplasser i SMB-bedrifter.	Velges av foreleseren fra del 1.3. [*Undervisningsmetoder, f.eks. praktiske oppgaver/laboratorier, spørrekonkurranser, spill, teknisk videoanalyse, casestudier, praktiske aktiviteter osv.*	Selvtest Kunnskapsvurderingstest

Kompetanse: Lærerne vil være kompetente i å utvikle og implementere strategiske cybersikkerhetsretningslinjer for SMB-arbeidsplasser	Velges av foreleseren fra del 1.3. [*Undervisningsmetoder, f.eks. konkurranser, CTF, simulerte miljøer, 5E, CBL, CL, PBL osv.]* i D2.3 *«Strukturen i læringsløpet for* SMB-cybersikkerhetsagenter»	Selvvalueringstester Kunnskapsvurderingstest

Modulens innhold: oversikt over emnene	Kontaktarbeidstimer					Individuelle arbeidstimer og oppgaver	
	Forelesninger (HEI)	Konsultasjoner	Praksis (HEI)	Tester	Alt kontaktarbeid	Individuelt arbeid	Oppgaver
Risikovurdering Generell risikostyringsprosess Generelt rammeverk for risikostyring Prinsipper for risikostyring Standarder for risikostyring Praktiske eksempler	2	0	2	0	**4**	5	Gi en kort oversikt over de viktigste trinnene i risikostyringsprosessen, inkludert risikoidentifisering, -vurdering og -kontroll. Definer de interne og eksterne kontekstene for risikostyring for en SMB. Spesifiser omfanget av risikovurderingen og identifiser viktige risikofaktorer. Utvikle risikokriterier som er spesifikke for den valgte SMB-bedriften.
Risikoidentifisering Lederskap og engasjement i risikostyring Definere omfanget av risikostyringsaktiviteter Ekstern og intern kontekst for risikostyringen Materielle og immaterielle risikokilder Årsaker og hendelser Trusler og muligheter Sårbarheter og evner Endringer i den eksterne og interne konteksten Indikatorer på nye risikoer Arten og verdien av eiendeler og ressurser Konsekvenser og deres innvirkning på målene Begrensninger i kunnskap og pålitelighet av informasjon	4	0	4	0	**8**	5	Identifiser både konkrete og abstrakte risikokilder for SME. Kategoriser risikoer basert på årsaker, hendelser, trusler og muligheter. Analyser SMEs interne sårbarheter og evner, og vurder hvordan endringer i både eksterne og interne kontekster kan påvirke virksomheten. Identifisere potensielle nye risikoer for SMB og foreslå indikatorer for å overvåke dem. Vurdere hvordan arten og verdien av eiendeler og ressurser påvirker denne analysen

Forutinntatte holdninger, antakelser og oppfatninger hos de involverte Praktiske eksempler og case-studier							
Trusler fra innsiden Definisjon og typer av trusler fra innsiden Kostnadene ved trusler fra innsidere Utarbeide et program for å redusere trusler fra innsiden Oppdage og identifisere interne trusler Vurdering av interne trusler Håndtering av interne trusler Praktiske eksempler og case-studier	6	0	6	0	**12**	5	Definer og klassifiser ulike typer interne trusler som er relevante for små og mellomstore bedrifter. Diskuter de potensielle kostnadene disse truslene kan påføre virksomheten. Utvikle et grunnleggende program for å redusere trusler fra innsidere for en SMB. Fremhev viktige komponenter som oppdagelse, identifisering og strategier for håndtering. Foreslå en metode for å vurdere interne trusler, og skissere tiltak for å håndtere disse truslene effektivt i en SMB-kontekst
Modeller og metoder for risikomåling og -evaluering Kvantitative og kvalitative risikovurderingsmodeller og -metoder Sannsynligheten for hendelser og konsekvenser Konsekvensenes art og omfang Kompleksitet og sammenheng Tidsrelaterte faktorer og volatilitet Evaluering av effektiviteten av eksisterende kontroller Sensitivitet og konfidensnivåer Praktiske eksempler og case-studier	6	0	6	0	**12**	5	Sammenlign og kontraster en kvantitativ og en kvalitativ risikovurderingsmodell. Vurder sannsynligheten for en risikohendelse og arten og omfanget av konsekvensene for en SMB. Vurder hvordan kompleksitet, tidsrelaterte faktorer og volatilitet påvirker denne vurderingen. Evaluer effektiviteten av gjeldende kontroller for håndtering av identifiserte risikoer. Inkluder en analyse av sensitivi-

							tets- og konfidensnivåer i kontrolltiltakene.
Risikokontroll Formulering og valg av risikohåndteringsalternativer Planlegging og implementering av risikobehandling Vurdere effektiviteten av denne håndteringen Avgjøre om den gjenværende risikoen er akseptabel Overvåking og gjennomgang Registrering og rapportering Praktiske eksempler og case-studier	6	0	6	0	**12**	5	Identifiser og velg passende risikohåndteringsalternativer for SME. Begrunn valget ditt ut fra arten av risikoen som er involvert. Utarbeid en kort risikohåndteringsplan som beskriver hvordan de valgte risikohåndteringsalternativene skal implementeres i en SMB-kontekst. Foreslå en metode for å vurdere effektiviteten av risikobehandlingen og avgjøre om den gjenværende risikoen er akseptabel.
Totalt	**24**	**2**	**24**	**0**	**50**	**25**	

Vurderingsstrategi	**Sammenlignende vektprosent**	**Vurderingskriterier**
Selvbedømmelsestest (1)	5	10 poeng – 95–100 % riktige svar. 9 poeng – 85–94 % riktige svar. 8 poeng – 75–84 % riktige svar. 7 poeng – 65–74 % riktige svar. 6 poeng – 55–64 % riktige svar. 5 poeng – 45–54 % riktige svar. 4 poeng – 35–44 % riktige svar. 3 poeng – 25–34 % riktige svar. 2 poeng – 15–24 % riktige svar. 1 poeng – 0–14 % riktige svar.
Selvtest (2)	5	
Selvvalueringstest (3)	5	
Selvtest (4)	5	
Selvtest (5)	5	
Kunnskapsvurderingstest	75	

	Studiemateriale *(Etternavn, forbokstav. (År, måned, dag). Artikkelens tittel. Tidsskrift/journal/avisens tittel, volumnummer (utgavenummer), sidetall for hele artikkelen, utgiver, URL)*
	Obligatorisk lesning
1.	Adarsh Nair og Greeshma M. R. (2023) Mastering Information Security Compliance Management : A Comprehensive Handbook on ISO/IEC 27001:2022 Compliance. Packt Publishing, Limited **https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30652023&**query=risk%20management
2.	Gregory J. Falco, Eric Rosenbach (2021) Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity. Oxford University Press, e-bok

3. Kristina Narvaez, Betty Simkins, John Fraser (2014) Implementering av risikostyring i bedrifter: Case-estudier og beste praksis. John Wiley & Sons
- ENISA (2022) Risikostyringsstandarder
4. Direktiv (EU) 2022/2555 fra Europaparlamentet og rådet av 14. desember 2022 om tiltak for et høyt felles nivå av cybersikkerhet i hele Unionen, som endrer forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972, og om oppheving av direktiv (EU) 2016/1148 (NIS 2-direktivet)
5. ISO 31000 Risikostyring – Retningslinjer

Anbefalt lesning

- Shobhit Mehta (2023) ISACA Certified in Risk and Information Systems Control (CRISC®) Exam Guide. Packt Publishing, Limited **https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30806680&query=risk%20management**
- Peter H. Gregory (2021) CISM-sertifisert informasjonssikkerhetsleder All-in-One eksamensguide. McGraw-Hill
- ISACA (2021) CRISC Review Manual 7. utgave. ISACA
- Forordning (EU) 2022/2554 fra Europaparlamentet og rådet av 14. desember 2022 om digital operasjonell robusthet for finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011

8. M8: FORRETNINGSKONTINUITET, KATASTROFEGJENOPPRETTING, HENDELSESHÅNDTERING OG PERSONALSIKKERHET

Modultittel	Modul
FORRETNINGSKONTINUITET, KATASTROFEGJENOPPRETTING, HENDELSESHÅNDTERING OG PERSONALSIKKERHET	

Foreleser(e)	Institusjon eller avdeling hvor modulen undervises

Undervisningsform	Språk
Ansikt til ansikt, online, blandet, konsultasjoner	*Engelsk, finsk, tyrkisk, norsk, litauisk, rumensk, fransk, polsk, spansk*

Forutsetninger
Ingen

Antall tildelte ECTS-poeng	Studentens arbeidsbelastning	Kontaktarbeidstimer	Individuelle arbeidstimer
3	75	5	25

Formål og læringsutbytte

Etter fullført kurs vil studentene være i stand til å utarbeide og administrere omfattende planer for forretningskontinuitet og katastrofegjenoppretting (BC/DR), utvikle et funksjonelt program for hendelseshåndtering og etablere en sterk og effektiv personalsikkerhetspolicy. Studentene vil lære hvordan de kan beskytte eiendeler, sikre at unødvendige tap unngås, forhindre driftsstans, unngå eller begrense krisesituasjoner og krisehåndteringsmiljøer.
Etter fullført kurs vil studentene være i stand til å skrive og overvåke den vedvarende implementeringen av en grundig håndbok for cybersikkerhet for SMB-er ved hjelp av avanserte cybersikkerhetsprinsipper og -teknologier integrert i samsvar med alle nasjonale og internasjonale lover. Studentene vil også følge opp håndhevelsen.

Læringsutbytte av modulen	Undervisnings- og læringsmetoder	Vurderingsmetoder
Kunnskap: Studentene vil få avansert kunnskap om hvordan man lager og implementerer en omfattende håndbok for cybersikkerhet på arbeidsplassen i SMB-bedrifter, som inneholder avanserte prinsipper for cybersikkerhet, de nyeste forsvarsmekanismene og overholdelse av nasjonal og internasjonal lovgivning og standarder innen hendelseshåndtering, forretningskontinuitet og personellsikkerhet.	Velges av foreleseren fra del 1.3. [Undervisningsmetoder] i D2.3 «Strukturen i læringsløpet for SMB-cybersikkerhetsendringsagenter».	Selvtest, kunnskapstest

Ferdigheter: Deltakerne vil få ferdigheter i å lage og vedlikeholde en håndbok for cybersikkerhet på arbeidsplassen i SMB-bedrifter, ved å bruke avanserte metoder for å vurdere risiko, utforme effektive strategier for risikostyring og hendelseshåndtering, og utvikle omfattende planer for forretningskontinuitet tilpasset organisasjonens behov.	Velges av foreleseren fra del 1.3. [Undervisningsmetoder] i D2.3 «Strukturen i læringsløpet for SMB-cybersikkerhetsagenter»	Selvtest, kunnskapstest
Kompetanse: Deltakerne vil være kompetente til å utvikle og implementere en håndbok for cybersikkerhet for SMB-bedrifter, lede sikkerhetsprosjekter og team på en effektiv måte, og sikre samsvar med organisasjonens mål og compliance-forpliktelser.	Velges av foreleseren, fra del 1.3. [Undervisningsmetoder] i D2.3 «Strukturen i læringsløpet for SMB-cybersikkerhetsagenter»	Selvvalueringstester, kunnskapstest

Modulens innhold: oversikt over emnene	**Kontaktarbeidstimer**					**Individuelle arbeidstimer og oppgaver**	
	Forelesninger (HEI)	Konsultasjoner	Praksis (HEI)	Tester	**Alt kontaktarbeid**	**Individuelt arbeid**	**Oppgaver**
Håndtering av sikkerhetshendelser - Definisjon og betydning av hendelseshåndtering i cybersikkerhet - Viktige komponenter i en effektiv gjenoppretting etter hendelser - Oversikt over vanlige cybersikkerhetstrusler (phishing, trusler fra innsidere) - Utvikling av beredskapsplan (IRP) - Roller og ansvar i beredskapsteamet - Simulering av hendelsen: gjennomføring av en øvelsesplan.	5	0,5	3	0,5	**9**	**5**	Utarbeid en detaljert beredskapsplan for SMB-bedriften din, inkludert roller, ansvar og tiltak som skal iverksettes ved en cybersikkerhetshendelse. Simuler en hendelse og gjennomfør en øvelse for å teste effektiviteten av planen.

Gjenoppretting etter katastrofer - Forstå katastrofegjenoppretting - Utarbeide en katastrofegjenoppprettingsplan - Roller og ansvar i katastrofegjenoppretting - Gjenopprettingstrinn etter katastrofe	5	0,5	3	0,5	**9**	**5**	Lag en katastrofeberedskapsplan som beskriver prosedyrer for gjenoppretting av IT-infrastruktur og data etter en katastrofe. Inkluder en tidsplan for gjenoppretting og tildel teammedlemmene ansvar for hver fase av prosessen.
Forretningskontinuitet - Forståelse av forretningskontinuitet - Utvikling av forretningskontinuitetsplan (BCP) - Roller og ansvar i forretningskontinuitet - Analyse av forretningspåvirkning - Testing og forbedring av BCP	5	0,5	3	0,5	**9**	**5**	Utarbeid en forretningskontinuitetsplan som sikrer at kritiske forretningsfunksjoner forblir operative under og etter en forstyrrelse. Identifiser viktige tjenester og ressurser, og skissere beredskapsstrategier for å opprettholde dem under ulike scenarier.
Sikkerhetsbevissthet, opplæring og utdanning - Forstå sikkerhetsbevissthet - Utvikling av sikkerhetsopplæringsprogram - Ansattes ansvar innen cybersikkerhet - Måling av effektiviteten av sikkerhetsbevissthet -	1	0,5	2	0,5	**4**	**1**	Utvikle et opplæringsprogram for sikkerhetsbevissthet for din SME, med fokus på viktige retningslinjer og beste praksis for cybersikkerhet. Gjennomfør en opplæringsøkt for ansatte og vurder deres forståelse gjennom spørrekonkurranser eller interaktive aktiviteter.

Sikkerhetspraksis ved ansettelser - Definere krav til sikkerhetsroller - Gjennomføring av bakgrunnssjekker - Intervjuer for sikkerhetskomponenter - Løpende evaluering og utvikling	1	0,5	2	0,5	**4**	**1**	Innfør sikkerhetsfokuserte ansettelsesrutiner, inkludert bakgrunnssjekker og intervjuspørsmål som er utformet for å vurdere kandidatenes bevissthet om cybersikkerhet. Lag en sjekkliste over viktige sikkerhetskvalifikasjoner og egenskaper for potensielle ansatte.
Sikkerhetsrelaterte oppsigelsesrutiner - Umiddelbar tilbakekalling av tilgang - Henting av data og enheter - Avslutningssamtale for sikkerhetsinnsikt - Varsle relevante team - Juridiske og compliance-hensyn	1	0,5	2	0,5	**4**	**2**	Utarbeid en sikker oppsigelsesprosedyre som inkluderer trinn for å tilbakekalle tilgang, gjenopprette selskapets eiendeler og gjennomføre avskjedsintervjuer. Implementer et simulert oppsigelsesscenario for å evaluere effektiviteten av prosedyren.
Tredjepartssikkerhet - Vurdering av tredjepartsrisiko - Due diligence ved valg av leverandør - Implementering av kontraster og sikkerhetskrav - Løpende overvåking og revisjon - Håndtering av hendelser og kommunikasjon	2	0,5	2	0,5	**5**	**2**	Identifiser potensielle risikoer knyttet til tredjepartsleverandører og lag en sjekkliste for sikkerhetsvurdering for å evaluere deres overholdelse av SMEs standarder for cybersikkerhet. Utarbeid en kontraktmal som inkluderer sikkerhetskrav og straffer for manglende overholdelse.

Sikkerhet i gjennomgangsprosesser - Inkorporere sikkerhet i gjennomganger - Gjennomføring av regelmessige sikkerhetsrevisjoner - Sårbarhetsvurdering og penetrasjonstesting - Gjennomgang etter hendelser	1	0,5	1,5	0,5	**3,5**	**2**	Utvikle en prosess for regelmessig gjennomgang og oppdatering av SMEs retningslinjer og prosedyrer for cybersikkerhet. Planlegg og gjennomfør en simulert revisjon for å sikre at alle sikkerhetstiltak er oppdaterte og i samsvar med relevante standarder.
Spesielle utfordringer knyttet til personvern for ansattes personopplysninger - Begrensninger i datainnsamling - Lagring og tilgangskontroll - Overholdelse av personvernbestemmelser - Datadeling og tredjeparter - Ansattes samtykke og rettigheter	2	0,5	2	0,5	**5**	**2**	Utarbeide en personvernpolicy for håndtering av ansattes personopplysninger, som sikrer overholdelse av personvernlovgivning og beste praksis. Gjennomføre en risikovurdering for å identifisere potensielle sårbarheter i måten ansattes data lagres og behandles på.
Totalt	**23**	**2**	**20,5**	**4,5**	**50**	**25**	

Vurderingsstrategi	**Sammenlignende vektprosent**	**Vurderingskriterier**
Selvbedømmelsestest (1)	5	10 poeng – 95–100 % riktige svar. 9 poeng – 85–94 % riktige svar. 8 poeng – 75–84 % riktige svar. 7 poeng – 65–74 % riktige svar. 6 poeng – 55–64 % riktige svar. 5 poeng – 45–54 % riktige svar. 4 poeng – 35–44 % riktige svar. 3 poeng – 25–34 % riktige svar. 2 poeng – 15–24 % riktige svar. 1 poeng – 0–14 % riktige svar.
Selvtest (2)	5	
Selvtest (3)	5	
Selvtest (4)	5	
Selvtest (5)	5	
Kunnskapsvurderingstest	75	

Studiemateriale *(Etternavn, første initial. (År, måned, dag). Artikkelens tittel. Tidsskrift/journal/avisens tittel, volumnummer (utgavenummer), sidetall for hele artikkelen, utgiver, URL)*

Obligatorisk lesning
- Gregory J. Falco, Eric Rosenbach (2021). *Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity*. Oxford University Press, e-bok. - Michael Wallace, Lawrence Webber (2017). *The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets.* AMACOM. - National Institute of Standards and Technology (NIST). *Contingency Planning Guide for Information Technology Systems*. NIST SP 800-34 Rev. 1. - Cochran, K.A. (2024). Incident Response, Business Continuity, and Disaster Recovery. I: Cybersecurity Essentials. Apress, Berkeley, CA. **https://doi.org/10.1007/979-8-8688-0432-8_14**
Anbefalt lesning
- ISACA (2023). *CISM Review Manual 15. utgave*. ISACA. - Peter H. Gregory (2021). *CISM Certified Information Security Manager All-in-One Exam Guide*. McGraw-Hill. - IT Governance (2022). *ISO 22301:2019 – Systemer for kontinuitetsstyring. Krav.* - M. Souppaya, L. Feldman, G. Witte [2024], Guide for Cybersecurity Incident Recovery, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology U.S. Department of Commerce - Ihab Hanna Sawalha [2021]. Synspunkter på forretningskontinuitet og katastrofegjenoppretting. International Journal of Emergency Services

VEDLEGG

MAL FOR SYLLABUS

MODULBESKRIVELSE

Modultittel	Modulens kode
...	

Foreleser(e)	Institusjon eller avdeling hvor modulen undervises
...	...

Undervisningsform	Språk
Ansikt til ansikt, online, blandet, konsultasjoner	*Engelsk, ...*

Forutsetninger
...

Antall tildelte ECTS-poeng	Studentens arbeidsbelastning	Kontaktarbeidstimer	Individuelle arbeidstimer
3	...	...	...

Formål og resultater av modulen		
...		
Læringsutbytte av modulen	**Undervisnings- og læringsmetoder**	**Vurderingsmetoder**

Tilrettelegge ressurser (utstyr, programvare, teknologi)
...

Modulens innhold: oversikt over emnene	Kontakt arbeidstid					Individuelle arbeidstimer og oppgaver	
	Forelesninger (HEI)	Konsultasjoner	Praksis (HEI)	Tester	**Alt kontaktarbeid**	**Individuelt arbeid**	**Oppgaver**
1							
…							
n							
Totalt							

Vurderingsstrategi	**Sammenlignende vektprosent**	**Vurderingskriterier**
Selvtest I		…
…		…
Selvtest n		…
Kunnskapsevalueringstest		…

Studiemateriale *(Etternavn, forbokstav. (År, måned, dag). Artikkelens tittel. Tidsskrift/journal/avisens tittel, volumnummer (utgavenummer), sidetall for hele artikkelen, utgiver, URL)*
Obligatorisk lesning
…
Anbefalt lesning
…

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau