Statsligt kompetenceforløb i cyber- og informationssikkerhed

DIGITALISERINGSSTYRELSEN

Overblik over forløbet

KICK-OFF

28. februar

kl. 9:00 - 15:00

Morgenmad fra kl. 8:30

Scandic Falkoner

MODUL 1

20 - 21 marts

Med overnatning

kl. 9:00 - 16:00

Comwell Holte

MODUL 2

24. april

kl. 9:00 - 16:00

Morgenmad fra kl. 8:30

Crowne Plaza

LÆRINGSGRUPPE

4. juni

kl. 9:00 - 16:00

Spil *Under angreb*

Digitaliseringsstyrelsen

Landgreven 4, 1301

København K

MODUL 3

4 - 5. september

Med overnatning

kl. 9:00 - 16:00

Comwell Holte

MODUL 4

2. oktober

kl. 9:00 - 16:00

Morgenmad fra kl. 8:30

Scandic Falkoner

DIGITALISERINGSSTYRELSEN

Program for kick-off arrangement

Formålet med kick-off er at rammesætte og introducere jer til forløbet. Vi vil på kick-off give tid til, at I kan lære hinanden at kende. Samtidig får I kendskab til det aktuelle trusselsbillede, samt relevante sårbarheder og udfordringer via oplæg fra PET og CFCS.

Hvor: Scandic Falkoner

Program

08:30-09:00 Ankomst og morgenmad
09:00-10:00 Velkomst v. Digitaliseringsstyrelsen og øvelse
10:00-10:15 Pause
10:15-11.00: Mødes i læringsgrupper/netværk
11.00-12.00: Oplæg v. CFCS
12:00-13:00 Frokost
13:00-14:00 Oplæg v. PET ”Sådan forebygger du spionage”
14:00-15:00 Øvelse og opsamling

DIGITALISERINGSSTYRELSEN

Modul 1-2: Statens informationssikkerhedsuddannelse

Få konkrete metoder og værktøjer til at identificere risici og håndtere sikkerheden i din organisation.

Praktisk

Modul 1: 20 - 21 marts, kl. 9:00 - 16:00. Med overnatning på konferencested mellem kursusdagene.
Hvor: Comwell Holte

Modul 2: 24. april, kl. 9:00 - 16:00.
Hvor: Crowne Plaza

Der vil være fuld forplejning alle dage.

Det får du på modulerne

1. Indsigt og praktisk træning i styring af informationssikkerhed, som matcher kravet om statslige myndigheders efterlevelse af ISO 27001.

2. En introduktion til risikostyringsmetodik, risikovurderinger og dokumentation samt redskaber til risikostyring i praksis.

3. Værktøjer til leverandørstyring, beredskabsstyring, audit og opfølgning i forhold til informationssikkerhed.

DIGITALISERINGSSTYRELSEN

Læringsmål og temaer

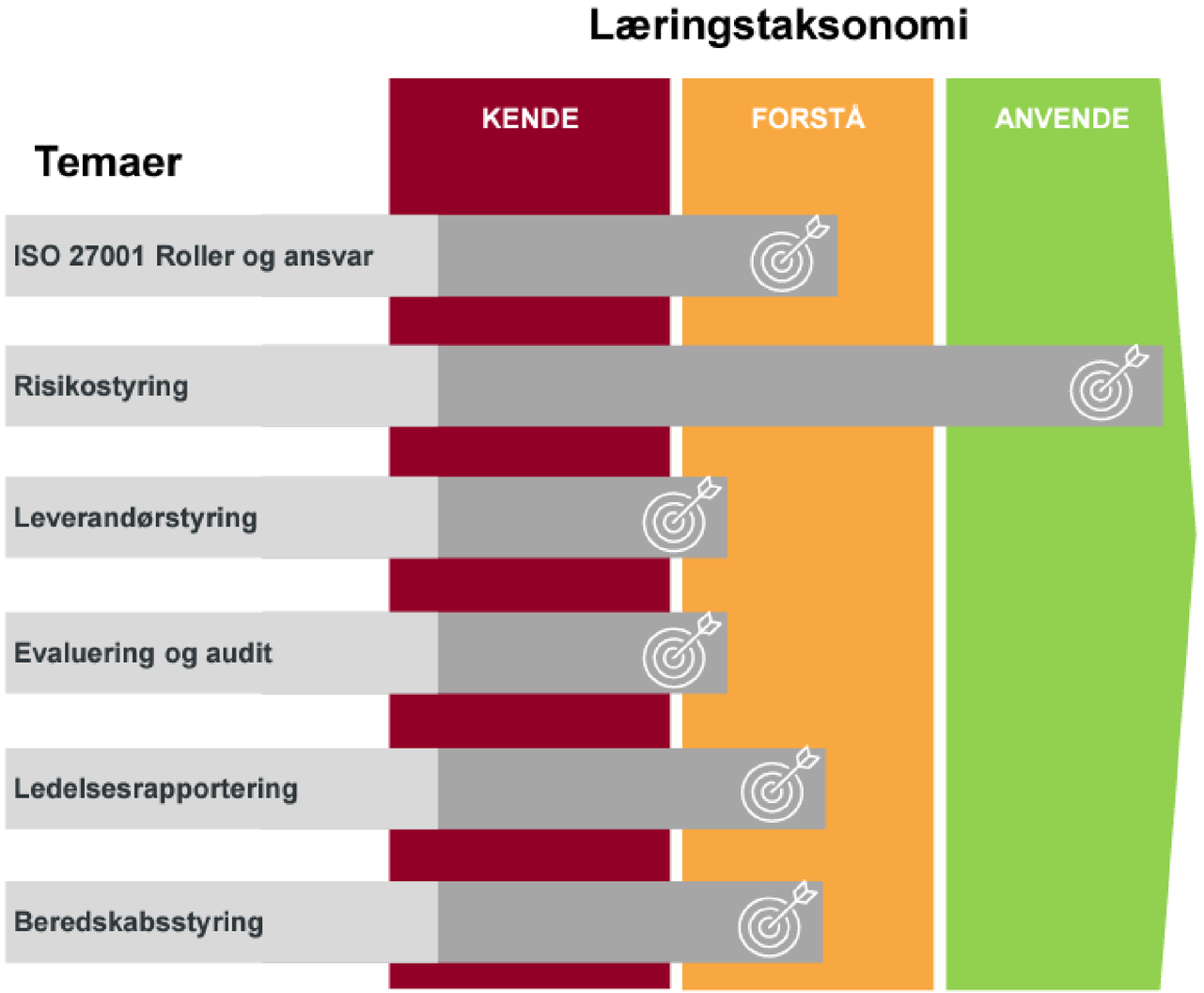
Overordnede læringsmål:

- Du sættes i stand til at kunne udpege relevante standarder og vejledninger, og du kan kortlægge roller og ansvar på tværs af aktiviteter, der berører risiko-og leverandørstyring samt evaluering.

- Du kan identificere, nedbryde og kvantificere et samlet risikooverblik med brug af de udleverede skabeloner og værktøjer.

- Du får en praktisk indføring i anvendelsen af forskellige metoder til at sikre den rigtige kontraktuelle regulering af informationssikkerheden i kontrakt med en leverandør.

- Du bliver introduceret til konkrete værktøjer til gennemførsel af evaluering, audit og ledelsesrapportering.



DIGITALISERINGSSTYRELSEN

Kursusprogram

Modul 1 - Dag 1

01: Sikkerhedsarbejdet i staten & ISO 27000landskabet

Myndighedernes arbejde med informationssikkerhed de seneste 10 år har givet øget modenhed i sikkerhedsarbejdet, men der er fortsat udfordringer. I introduktionen gives et overbliksbillede med udgangspunkt i ISO-modenhedsanalysen samt nedslagspunkter i de største udfordringer.

02: **Roller og ansvar i staten**

Med udgangspunkt i en praktisk anvendelig model klædes I på til at kunne forstå roller og ansvar i informationssikkerhedsarbejdet i staten.
Praksisøvelser sikrer drøftelse af, hvilke roller I ser i jeres eget arbejde, inklusive om alle roller og ansvar er placeret og efterlevet i jeres organisation.
Der vil være fuld forplejning alle dage.

03: Risikostyring i praksis

I arbejder konkret med forskellen på trusler, sårbarheder og risici samt sandsynlighed og konsekvens. Dette gøres med udgangspunkt i konkrete eksempler, som I vil kunne genkende fra jeres hverdag, og som typisk kan være svære at definere.

Modul 1 - Dag 2

04: Leverandørstyring

I præsenteres for faserne i leverandørstyring før, under og efter, og I skal på baggrund heraf anvende centrale vejledninger i relation til casearbejdet senere på dagen

05: **Ekspertoplæg om leverandørstyring**

Ekspertoplæg sætter fokus på den praktiske anvendelse af vejledninger og håndtering af leverandørstyring. Oplægget giver således konkrete eksempler på arbejdet med cyber-og informationssikkerhed i leverandørforholdet.

06: Audit, evaluering og opfølgning

Via oplæg og praksisnære øvelser oparbejder I viden om processen for god evaluering, audit og opfølgning. Herigennem opnår I fortrolighed med anvendelse af centrale skabeloner og vejledninger, som kan tages i anvendelse i egen organisation efter uddannelsesforløbet.

Modul 2 - Dag 3

07: Ledelsesrapportering i sikkerhedarbejdet

I arbejder ved denne del af uddannelsen med udarbejdelse af ledelsesrapportering efter kort introduktion til, hvad ledelsesrapportering er, og gennemgang af praktiske råd og gode principper for arbejdet med dette.

08: **Håndtering af krisesituation**

Øvelsen er en praksisnær træningsøvelse, hvor I bliver bevidste om, hvad de skal gøre i krisesituationer, samt hvilke huller I har i jeres nuværende viden og evt. praksis i egen organisation. I bliver bevidste om formålet med de forskellige redskaber fx beredskabsplaner og risikovurderinger.

09: Beredskabsstyring

I får en forståelse for organisering, nøgleaktiviteter og -begreber inden for beredskabsplanlægning samt et overordnet kendskab til de konkrete redskaber til støtte af et samlet beredskab.

DIGITALISERINGSSTYRELSEN

Læringsgruppe

Spil *Under angreb*

- Den 4. juni 2024
- Hos Digitaliseringsstyrelsen - Landgreven 4, 1301 København K
- kl. 13:00 - 15:00
- I deles op i grupper, hvor I spiller spillet Under angreb faciliteret af Center for Cybersikkerhed
- Kort om spillet: Under Angreb fører spillerne gennem to år i en fiktiv virksomhed med trusselsanalyse, sårbarhedsanalyse, handlingsplaner og reaktioner på angreb. Spillet giver mulighed for at arbejde operationelt med cybersikkerhed og afrundes med at deltagerne tager de første skridt i retning af deres egen handlingsplan. Spillet er udviklet i af Copenhagen Game Lab i samarbejde med Center for Cybersikkerhed.

Modul 3-4: Teknisk it-sikkerhed i staten

Få dyb it-sikkerhedsteknisk viden via kontektsnære case-øvelser og eksempler fra en statslig virkelighed

Praktisk

Modul 3: 4 - 5 september, kl. 9:00 - 16:00. Med overnatning på konferencested mellem kursusdagene.
Hvor: Comwell Holte

Modul 4: 2. oktober, kl. 9:00 - 16:00.
Hvor: Scandic Falkoner

Der vil være fuld forplejning alle dage.

Det får du på modulerne

1. Evnen til at vurdere, udfordre og kvalitetssikre den konkrete implementering af de obligatoriske tekniske minimumskrav

2. Styrkelse af din forståelse for trusselsbilledet og de relevante aktører gennem arbejde med threatmodelling

3. Forståelse for grundlæggende elementer og komponenter i sikkerhedsarkitekturen

4. Rustes til at indgå i et sikkerhedsteknisk leverandørsamarbejde og kunne stille de nødvendige krav

5. Indsigt i sikkerhedsforhold, udfordringer og muligheder når det kommer til brug af cloud

6.Styrkelse af din kommunikation med forretningen ved implementering af tekniske sikkerhedsforanstaltninger

DIGITALISERINGSSTYRELSEN

Læringsmål og temaer

Overordnede læringsmål:

- *Trusler og risikostyring*

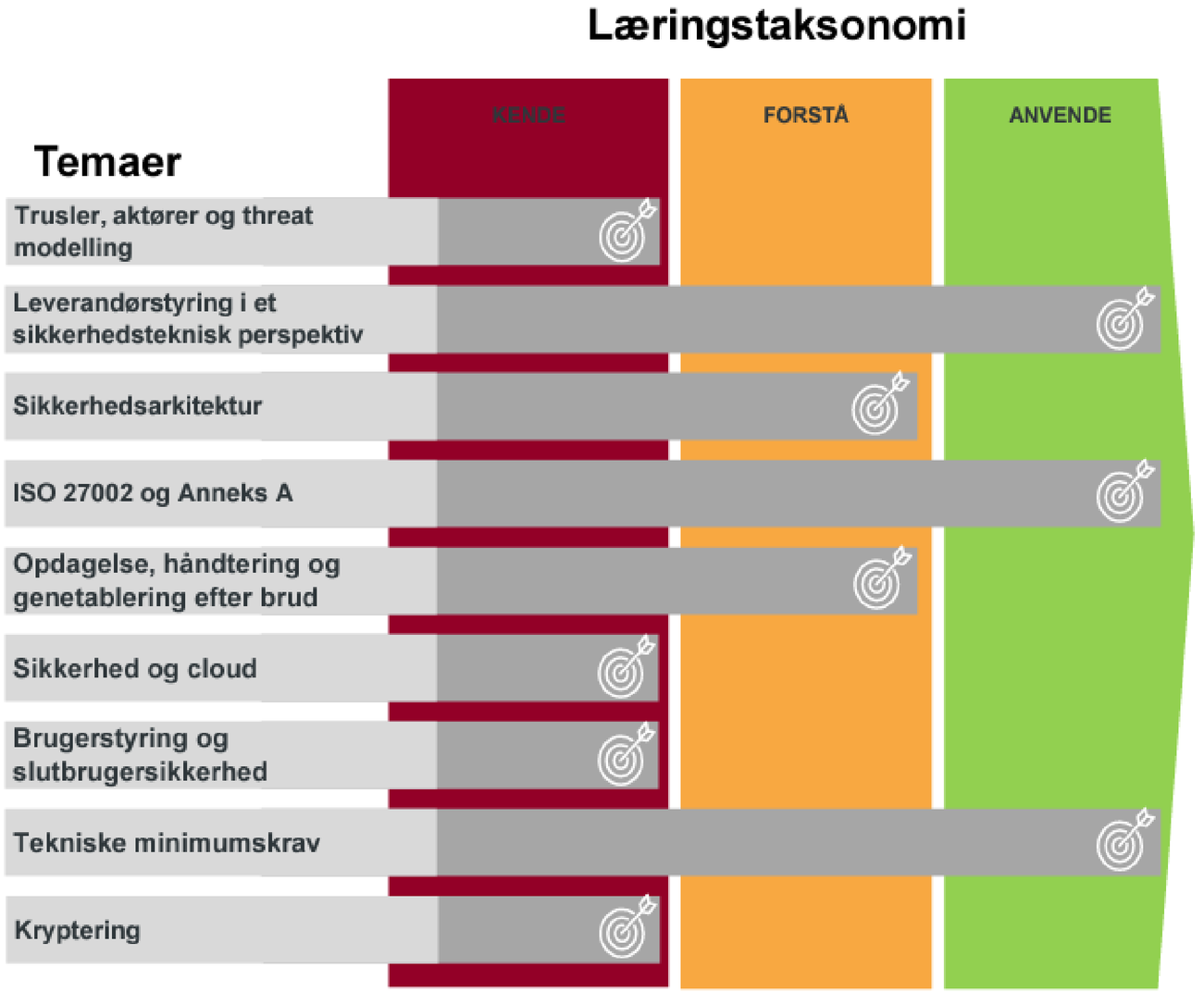
Du rustes til at forstå trussels billedet, inkl. aktørernes virkemidler. Du introduceres til og arbejdermed metoder til threat modelling.

- *Teknisk it-sikkerhed i praksis*

Du styrkes i at kunne løfte din rolle og ansvar i arbejdet med teknisk it-sikkerhed i egen organisation. Du arbejder med bl.a. sikkerhedsarkitektur og kryptering.

- *Forberedelse og håndtering af krisesituationer*

Du styrkes i at kunne løfte din rolle og ansvar i arbejdet med teknisk it-sikkerhed i egen organisation. Du arbejder med bl.a. sikkerhedsarkitektur og kryptering.



DIGITALISERINGSSTYRELSEN

Kursusprogram - Modul 3

Dag 1

01: Rammer for it-sikkerhed i staten
I første modul får deltagerne indsigt i de strategiske og lovgivningsmæssige rammer for it-sikkerhed i staten. Vi berører bl.a. ISO 27002, der er kommet i en dansk udgave i 2023 og kommer kort ind på NIS2 og dennes betydning.

02: **Trussler, aktører og threat modelling**
Her får deltagerne indsigt i den nyeste viden om trusler mod offentlige myndigheder. Der er særligt fokus på trusselsaktørerne og de virkemidler, de anvender gennem praktiske øvelser med threatmodellingog MitreATTACK & DEFEND

03: Sikkerhedsarkitektur
Efter frokost på dag 1 bliver deltagerne gennem forståelse for relevante sikkerhedsarkitekturer rustet til at være kravstillere og sparringspartnere til itorganisation og løsningsleverandør ved valg af sikkerhedsarkitekturer.

04: Opdagelse, håndtering & genåbning efter sikkerhedsbrud
Cybersikkerhedshændelseri kontinuerlig udvikling stiller nye og udvidede krav til deltagernes forståelse af den traditionelle håndtering af it-sikkerhedsbrud. Gennem praktiske og kontekstnære øvelser får deltagerne viden om kritiske processer og tekniske redskaber før, under og efter et sikkerhedsbrud uanset karakteren af sikkerhedsbruddet.

Dag 2

05: Brugerstyring og slutbrugerssikkerhed
I præsenteres for faserne i leverandørstyring før, under og efter, og I skal på baggrund heraf anvende centrale vejledninger i relation til casearbejdet senere på dagen

06: Sikkerhedskultur II: Kryptering
Deltagerne får her viden på højt niveau om, hvordan kryptering virker, og i hvilke situationer centrale krypteringsmetoder er effektive. Deltagerne bliver dermed i stand til at stille de rette krav til tekniske løsninger og infrastruktur.

07: Sikkerhedsarkitektur III: Cloud og sikkerhed
Gennem fortsat arbejde med den fiktive case-applikation, som nu er blevet flyttet til skyen, får deltagerne indsigt i cloud-sikkerhed i relation til sikkerhedsarkitektur, brugsmønstre og ikke mindst faldgruber.

08: Leverandørstyring i et sikkerhedsteknisk perspektiv
Som informationssikkerhedsmedarbejder i staten er det afgørende at kunne bidrage til en tilstrækkelig leverandørstyring på de tekniske områder –særligt på områder med stor innovation som fx cloud, IOT, virtualisering, containere og mobile løsninger.

08: Tekniske minimumskrav
Vi sætter deltagerne i stand til at evaluere og føre tilsyn med tilstrækkeligheden i opfyldelsen af de tekniske minimumskrav gennem en dyb og praktisk forståelse for kravene og implementeringen af dem.

DIGITALISERINGSSTYRELSEN

Kursusprogram - Modul 4

01: Opsummering af pensum, samt besvarelse af tvivlsspørgsmål
IElevpræsentationer kombineret med elevernes nye erfaringer. Mulighed for besvarelse af spørgsmål, der er opstået i det praktiske arbejde med informationssikkerhed undervejs i forløbet.

02: **Kill Chain teori og øvelser**
Deltagerne lærer at tænke som en hacker gennem teori og øvelser om Kill Chain. Ved at forstå killchain-modellen kan styrelser, ministerier og departementer bedre beskytte sig mod cyberangreb, ved at implementere sikkerhedsforanstaltninger på hver af disse faser. Ved at afbryde angriberens progression gennem modellen kan man reducere risikoen for succesfulde angreb.

03: Live-hacking
lVed at se en hacker i aktion kan man fx lære om nogle af de mest almindelige sårbarheder og angrebsmetoder relateret til den offentlige sektor. Dette kan hjælpe kursusdeltagerne med at forstå, hvad en angriber er i stand til, har nemt ved og hvilke begrænsninger der er. Ligeledes er der mulighed for at stille spørgsmål til, hvordan en hacker tænker, mv.

04: Statslig oplægsholder
Oplæg fra en statslig oplægsholder om et cyberangreb/hændelse og hvad der blev gjort. Skal give praktisk viden til deltagerne og inspiration til konkret anvendelse af værktøjer fra kurset. Opsamling, afrunding og evaluering*

**Der tages forbehold for mindre ændringer i programmet*

DIGITALISERINGSSTYRELSEN