INDENRIGS- OG SUNDHEDSMINISTERIET

Slotsholmsgade 10-12
DK-1216 København K

T +45 7226 9000
F +45 7226 9001
M sum@sum.dk
W sum.dk

Dato: 19-08-2025
Enhed: ISDB-enheden
Sagsbeh.: HBN
Sagsnr.: 2025-4562
dokumentnr.: 9186167

Udvalg for Cyber-, og informationssikkerhed og databeskyttelse (CID-udvalg)

Referat for møde i CID-udvalg 2-2025

Dato for møde
29. august 2025

Deltagere
Medlemmer
Cecilie Louise Svane Olesen (CLSO), forperson
Annette Baun Knudsen (ABKN), ISDB & IT
Trine Brøbecher (TRBR), HR
Pernille Seaton (PSE), Intern Administration
Lene Jensen (LRJ), IT

Observatør
Helle Ginnerup-Nielsen (HGN), DPO DEP

Ressourcepersoner
Frederik Kastoft-Davidsen (FKD), ISDB
Mette Rye Andersen (MRAN), ISDB

Sekretariat
Helga Brask Nielsen (HBN), DPA

Indhold

Dagsorden

1. Velkomst

v/CLSO

Sagsfremstilling

ISO 27001:2023-standarden, NIS 2-loven og GDPR stiller krav om, at departementet etablerer en risikostyringsproces, der sikrer, at relevante processer og systemer risikovurderes og håndteres.

ISDB har udarbejdet udkast til tre styringsdokumenter: Politik for risikostyring, der fastlægger rammer, krav og forankring af risikostyring, Retningslinje for risikostyring, der beskriver metode, roller, ansvar og risikotolerance samt Konsekvens- og sandsynlighedstabeller, der angiver skalaer til brug for vurdering af sikkerhedsrisici. Se vedlagt bilag for et overblik.

Bilag

1.1. Overblik over implementering af risikostyring i departementet

Gennemgang

CLSO bød velkommen og rammesatte i den forbindelse mødets formål og baggrund, navnlig implementering af risikostyring i departementet og mere specifikt godkendelse af politik for risikostyring, retningslinje for risikostyring og konsekvens- og sandsynlighedsskalaer. CLSO bemærkede, at grundet mødets emnespecifikke fokus, så var de sædvanlige CID-udvalgsdagsordenspunkter ikke med på dette møde.

CLSO gav ordet til FKD, der i overensstemmelse med den fremsendte dagsorden gennemgik hhv. politik for risikostyring, retningslinje for risikostyring og konsekvens- og sandsynlighedsskalaer.

Følgende væsentlige pointer blev fremlagt på mødet:

TRBR bemærkede, at det ifm. implementering af risikostyring i departementet er vigtigt, at ISDB er opmærksomme på, at indholdet af styringsdokumenterne skal formidles til huset, fx i forbindelse med undervisning på kontormøder. TRBR bemærkede endvidere, at det er vigtigt, at organisationen ved at de skal henvende sig til ISDB inden ibrugtagning af nye systemer eller iværksættelsen af nye behandlingsaktiviteter. FKD oplyste, at ISDB i dag informerer herom ad hoc, fx i forbindelse med onboarding af nye medarbejdere, og at spørgsmålet desuden vil blive behandlet i en retningslinje for erhvervelse, som er et NIS 2-krav.

ABKN orienterede om ISDB's overvejelser om implementering og formidling, herunder at der er planer om at bygge et complianceunivers på intranettet, udarbejdelse af en one-pager med information omkring forventninger i forbindelse med risikoejerskab suppleret med direkte information og vejledning til proces- og systemejere, som har særlige roller i risikostyringsprocessen.

HGN bemærkede, at styringsdokumenterne der var til godkendelse i dag kun omhandler sikkerhedsrisiko ift. informationssikkerhed og at vurderingen om høj risiko i GDPR skal være en supplerende vurdering, som skal håndteres i en anden proces. FKD bemærkede, at de efterspurgte vurderinger i forhold til GDPR ville blive behandlet i forbindelse med legalitetsvurderinger og at legalitetsvurderinger ville blive udarbejdet i forbindelse med opdatering af departementets fortegnelser over behandlingsaktiviteter. ISDB har

udarbejdet en skabelon til legalitetsvurderinger, der har været anvendt i forbindelse med systemer, der er taget i brug i HR. HGN bemærkede desuden, at der ved fastlæggelse af risikotolerance ikke er samme råderum for accept af risiko i GDPR, som ved de andre risikotyper.

FKD oplyste afslutningsvis, at implementering af politikker og retningslinjer vil medføre et betydeligt ressourcetræk særligt for ISDB og IT, men også for procesejere og risikoejere i øvrige kontorer/centre i departementet.

2. Godkendelse af politik for risikostyring

v/FKD

Indstilling
Det indstilles,
at CID-udvalget godkender politik for risikostyring.

Sagsfremstilling
Politik for risikostyring er en emnespecifik politik, der fastsætter det overordnede omfang for risikostyringen af informationssikkerhed i departementet. Behovet for at implementere emnespecifikke politikker er forankret i nye krav i forbindelse med overgangen fra ISO 27001:2013- til ISO 27001:2023-standarden samt krav i NIS 2-loven.

Politik for risikostyring omhandler styring og forankring af ledelsens krav til risikostyring i departementet:

- Hvilke lovkrav risikostyringen skal omfatte? (GDPR og NIS 2-loven)
- Hvilke aktiver skal risikostyres i departementet? (processer og systemer)
- Hvilke interessenter og risikoejere er ansvarlige for risikostyring i departementet? (ISDB & IT, proces- og systemejer)
- Hvilke typer af brud skal der vurderes i forhold til? (fortrolighed, integritet, tilgængelighed og autenticitet)
- Hvem konsekvenser skal vurderes for? (departementet, den registrerede og samfundet)
- Hvordan håndteres identificerede risici? (accept, modificer, del og/ eller undgå)
- Hvordan og med hvilken frekvens rapporteres risikobilledet til ledelsen? (en gang årligt)

Bilag
2.1. Politik for risikostyring – Udkast

Videre proces
Politik for risikostyring vil efter godkendelse blive offentliggjort på intranettet.

Beslutning
CID-udvalget godkendte politik for risikostyring, herunder den videre proces.

3. Godkendelse af retningslinje for risikostyring

v/FKD

Indstilling
Det indstilles,
at CID-udvalget godkender udkast til retningslinje for risikostyring.

Sagsfremstilling
Retningslinje for risikostyring er en detaljeret udmøntning af departementets krav til risikostyring, jf. Politik for risikostyring. Retningslinjen indeholder således metode, roller og ansvar i forhold til at foretage risikovurdering og risikohåndtering samt risikotolerance. Det bemærkes, at risikotolerancen vil blive beskrevet i retningslinjen, når direktionen har godkendt risikotolerancen, jf. proces for fastlæggelse af risikotolerance, som fremgår af punkt 5 a.

Det bemærkes yderligere, at den proces, som er beskrevet i retningslinjen, allerede har været anvendt ifm. udarbejdelsen af en række risikovurderinger, heriblandt risikovurdering af auto-complete i Boxer og Outlook, risikovurdering af Plandisc, risikovurdering af departementets fællesdrev F- og G-drevet.

Bilag
3.1. Retningslinje for risikostyring – Udkast

Videre proces
Retningslinje for risikostyring vil efter godkendelse blive offentliggjort på intranettet.

Beslutning
CID-udvalget godkendte retningslinje for risikostyring, herunder den videre proces.

4. Godkendelse af konsekvens- og sandsynlighedsskalaer
v/FKD

Indstilling
Det indstilles,
at CID-udvalget godkender udkast til konsekvens- og sandsynlighedsskalaer.

Sagsfremstilling
Konsekvens- og sandsynlighedstabeller anvendes til at vurdere risikoen for at en hændelse indfinder sig i en proces eller et system. Det udføres konkret ved at enkelte risikoscenarier scores for konsekvens og sandsynlighed.

Vedlagte bilag omfatter følgende skalaer udviklet til risikovurdering af sikkerhedsrisiko i departementet.

Skala	Risikoobjekt for konsekvens	Regulatorisk kontekst	Afstemt med
Databeskyttelse	Den registrerede	ISO/IEC 27701:2019, GDPR	DPO, DPA samt ISDB & IT
Omdømme	ISM-DEP	ISO/IEC 27001:2023	Presse og Kommunikation
Operationel/ Administrativ	ISM-DEP	ISO/IEC 27001:2023	ISDB & IT, HR
Økonomisk	ISM-DEP	ISO/IEC 27001:2023	Koncernøkonomi
Borgere	Samfundet	NIS 2	De koncernfælles referencerammer for konsekvensvurdering
Samfundsøkonomien	Samfundet	NIS 2	De koncernfælles referencerammer for konsekvensvurdering

Sandsynlighed	Den registrerede, ISM-DEP, samfundet	ISO/IEC 27001:2023, ISO/IEC 27701:2019, GDPR, NIS 2	ISDB & IT

ISDB har i forbindelse med udarbejdelse af udkastet afholdt møder med de respektive organisatoriske enheder i departementet, for hvem de enkelte skalaer har været mest relevant. På møderne har de enkelte fagkontorer kvalificeret og revideret skalaerne.

Det bemærkes, at konsekvens- og sandsynlighedstabellerne ligeledes har været anvendt i departementet til udarbejdelsen af en række risikovurderinger, bl.a. auto-complete i Boxer og Outlook, risikovurdering af Plandisc, risikovurdering af departementets fællesdrev F- og G-drevet.

Bilag
4.1. Konsekvens- og sandsynlighedsskalaer – Udkast

Videre proces
Konsekvens- og sandsynlighedsskalaer vil efter godkendelse blive offentliggjort på intra-nettet.

Beslutning
CID-udvalget godkendte konsekvens- og sandsynlighedsskalaer, herunder den videre proces for implementering.

Det bemærkes i den forbindelse, at i overensstemmelse med dagsordenen, ville risikotolerancen blive indført i retningslinje for risikostyring efter godkendelse af direktionen og at denne indførsel ikke ville kræve yderligere godkendelse af retningslinje for risikostyring.

5. Orienteringspunkter

5.a Orientering om proces for fastlæggelse af risikotolerance
v/FKD

Indstilling
Det indstilles,
at CID-udvalget tager orienteringen til efterretning

Sagsfremstilling
Risikotolerance er et centralt element i styring af risici i relation til cyber, informationssikkerhed og databeskyttelse. Risikotolerancen er det niveau af risiko, som departementet er villigt til at acceptere, uden at der kræves yderligere risikohåndtering med henblik på at beskytte departementets informationer.

Det er et krav ifølge NIS 2-loven og best pratice, at risikotolerancen besluttes af den øverste ledelse, dvs. direktionen.

Fastlæggelsen af departementets risikotolerance indebærer, at der skal etableres en række tærskler, som her foreslås at være: Lav, mellem, høj og meget høj. For hver tærskel, vil der være tilknyttet en beskrivelse af, hvor hurtigt departementet skal reagere på de identificerede risici, og på hvilket ledelsesniveau risikoen kan accepteres.

Det er muligt for departementet at have forskellige risikotolerancer for forskellige typer af risici, f.eks. risiko for den registrerede, risiko for departementet og risiko for samfundet.

Følgende overordnede proces er besluttet til fastlæggelse af risikotolerancen:

1. CID-udvalget udarbejder et udkast til risikotolerance
2. Risikotolerance godkendes af direktionen

Ad. 1: Proces for udarbejdelse af udkast til risikotolerance
ISDB faciliterer en 2-timers workshop med CID-udvalgets medlemmer med henblik på at udarbejde et udkast til risikotolerance, som efterfølgende kan godkendes af direktionen.

Workshoppen indledes med en kort introduktion, hvorefter der gennemføres en øvelse, hvor deltagerne vurderer eksempler på risici med forskellige risikoniveauer. På baggrund af workshoppen udarbejdes et udkast til, hvilke risici der kan accepteres på hvert niveau (lav, mellem, høj, meget høj). Afslutningsvis afklares, hvilke ledelsesniveauer der skal have kompetence til at acceptere de forskellige risikoniveauer.

Workshoppen skal resultere, at CID-udvalget godkender et konkret og operationelt udkast til risikotolerance og ansvar, som kan forelægges direktionen til godkendelse.

Ad. 2: Proces for godkendelse af udkast til risikotolerance i direktionen
CID-udvalgets udkast til risikotolerance forelægges direktionen til godkendelse i forlængelse af den interne undervisning af direktionen i NIS 2 og cybersikkerhed, som skal finde sted i løbet af efteråret 2025, jf. vedlagt cover som bilag.

Bilag
5.1. Cover af 8 august vedr. intern undervisning af ledelsen i NIS 2 og cybersikkerhed 2025.

Videre proces
ISDB udarbejder materiale og program til afholdelse af en workshop til udarbejdelse af et udkast til risikotolerance.

CID-udvalget indkaldes til en 2-timers workshop til udarbejdelse af et udkast til risikotolerance en dag i uge 38 til 40.

Direktionen inviteres til intern undervisning i NIS 2 og cybersikkerhed i efteråret, hvor udkast til risikotolerance godkendes.

Fastlagt risikotolerance indføres i retningslinje for risikostyring.

Beslutning
CID-udvalget tog orienteringen til efterretning.

6. Eventuelt

Der var intet under eventuelt.

7. Næste møde
Afholdes torsdag den 16. september 2025 kl. 10.00-11.30