FORSVARSMINISTERIET

Forsvars-ministeriets informations-sikkerhedsstrategi 2018-2020

Indhold

1. Forord af departementschefen

Danmark er et af de mest digitaliserede lande i verden, og vores fortsatte vækst og velfærd er i meget høj grad afhængig af, at vi som nation kan sikre vores informationer og de teknologier, vi anvender til at behandle vigtige informationer.

Gennem de seneste år har vi oplevet en række cyberangreb mod danske myndigheder, virksomheder og borgere, hvoraf nogle bl.a. har medført store økonomiske tab.

Vi ser i dag generelt flere sårbarheder i it-systemerne, bl.a. fordi mange systemer nu kan tilgås fra internettet, hvor systemer og komponenter tidligere var isoleret på interne, lukkede netværk. Det er muligt at finde frem til værktøjer og teknikker på internettet, som udnytter sårbarheder i software og it-systemer, og disse former for angreb er blevet langt mere almindelige.

Forsvarsministeriet har en central rolle i forsvaret af Danmark, også i forbindelse med forsvaret mod ødelæggende cyberangreb mod danske interesser i bred forstand. Vi har et ansvar over for vores internationale alliancepartnere for at leve op til aftaler og krav til sikring af den information, som vi deler med hinanden. Denne rolle og dette ansvar udgør grundlaget i denne informations-sikkerhedsstrategi.

Informationssikkerhedsstrategien skal binde Forsvarsministeriets it-strategi og øvrige koncernfælles forretningsstrategier sammen med styrelsernes egne forretningsstrategier og dermed sikre grundlaget for en overordnet prioritering og styring.

Forsvarsministeriets informationssikkersstrategi udtrykker de visioner, prioriteringer og initiativer, som vi vil gennemføre i denne kommende tre-års periode med henblik på at kunne leve op til koncernens ansvar.

Forsvarsministeriets informationssikkerhedsstrategi er ambitiøs og den væsentligste målsætning er at gøre koncernen yderligere robust over for potentielle angreb såvel som over for situationer, når angreb rammer.

Herudover udtrykker strategien de nyeste principper for informationssikkerhed og dermed den retning, som koncernledelsen vil styre efter fremover.

Informationssikkerhedsstrategien henvender sig dermed til alle ansatte i koncernen såvel som til interessenter og samarbejdspartnere inden for andre sektorer i det danske samfund.

God læselyst!

Thomas Ahrenkiel
Departementschef

2. Om informationssikkerheds-strategiens tilblivelse

Det militære sikkerhedsområde ekskl. informationssikkerhed er forankret i Forsvarsministeriets Sikkerhedsudvalg, mens informationssikkerhedsområdet er forankret i Koncernfælles Informationssikkerhedsudvalg (KIU). Forsvarsministeriet varetager governanceniveauet for informationssikkerhedsområdet, og Koncernfælles Informationssikkerhedsudvalg refererer til Forsvarsministeriet. Forsvarets Efterretningstjenestes Center for Cybersikkerhed varetager opgaven som national it-sikkerhedsmyndighed og som koncern it-sikkerhedsmyndighed.

Udarbejdelsen af informationssikkerhedsstrategien er igangsat med Koncernfælles Informations-sikkerhedsudvalg som styregruppe og udført i en tværgående arbejdsgruppe med deltagere fra alle styrelser. Det har været et mål, at alle styrelser har været tæt involveret i arbejdet, fordi informations-sikkerhedsstrategien understøtter det fælles perspektiv såvel i forhold til Forsvarsministeriets it-strategi, øvrige strategier som i forhold til styrelsernes egne forretningsmæssige strategier.

Der skal rettes en stor tak til medlemmerne af den tværgående arbejdsgruppe, der har arbejdet med strategien.

3. Visioner for informations-sikkerhedsstrategien

På informationssikkerhedsområdet har Forsvarsministeriet defineret fem visioner, der alle skal sætte retning og sikre, at informations-sikkerheden i koncernen understøtter og realiserer koncernens strategiske målbillede.

Forsvarsministeriets visioner er, at:

1. **Sikre et effektivt cyberforsvar og -beredskab**
   Vi skal være i stand til at reagere, når angreb rammer vores systemer og vores brugere. Til forskel fra "beskyttelse", definerer vi i denne sammenhæng "forsvar", som vores evne til at handle reaktivt, når angreb rammer os.

2. **Beskytte internetvendte systemer mod cyberangreb**
   Vi vil beskytte internetvendte systemer. Det vil sige systemer på netværk, hvorfra der er adgang til internettet. I denne sammenhæng definerer vi "beskytte", som det at handle proaktivt inden et angreb rammer, ved at etablere foranstaltninger, der skal reducere risikoen for, at angrebet kan ramme.

3. **Styrke styring og ledelse af informationssikkerhed**
   Vi skal sikre, at styring af informations-sikkerheden er forankret i koncernledelsen og myndighedernes ledelser. Organiseringen skal understøtte, at de relevante ledelsesniveauer kan fastlægge informationssikkerhedsmål, som er koordinerede både horisontalt og vertikalt, herunder fastlægge koordinerede processer, hvorved målene kan realiseres.

4. **Arbejde helhedsorienteret med risikostyring**
   Vi skal tage udgangspunkt i løbende vurderinger af risici frem for faste regler samt tage hensyn til eventuelle gensidige afhængigheder, når vi tager stilling til vores risikovillighed. Når en myndighed beslutter sin risikovillighed, kan beslutningen have konsekvenser både vertikalt og horisontalt. De vertikale konsekvenser rammer f.eks. over- og underordnede myndigheder samt leverandør- og forsynings-kæder. Horisontalt set, kan beslutningen have betydning for sideordnede myndigheder inden for koncernen.

5. **Være ambitiøs og praksissættende**
   Vi vil være blandt de bedste til informations-sikkerhed i Danmark og dermed være et eksempel til efterfølgelse.

Disse visioner har et tidsperspektiv ud over den periode, som denne strategi omhandler. Derfor har

Forsvarsministeriet, med afsæt i visionerne, defineret en række prioriteringer, som sætter relevante rammer for de konkrete initiativer, der skal realiseres i strategiperioden:

1. **Prioriteringer i 2018-2020 angående visionen om at "Sikre et effektivt cyberforsvar og -beredskab":**

   - Cyberforsvarsindsatsen i forhold til koncernens internetvendte systemer skal styrkes.
   - Det skal sikres, at koncernen besidder et aktivt og effektivt beredskab, når angreb rammer.
   - Alle medarbejdere gennemgår awareness og træning i relation til funktion og opgaver, så de er opmærksomme, når angreb rammer.

2. **Prioriteringer i 2018-2020 angående visionen om at "Beskytte internetvendte systemer mod cyberangreb":**

   - Gennem konsolidering af it-arkitekturen og proaktive sikkerhedstiltag vil vi reducere angrebsfladen mod koncernens internetvendte systemer.
   - Vi vil gøre det muligt for os selv at kunne udnytte de nyeste sikkerhedsteknologier bl.a. gennem løbende tilpasning af it-arkitektur og interfaces.

3. **Prioriteringer i 2018-2020 angående visionen om at "Styrke styring og ledelse af informationssikkerhed":**

   - Informationssikkerhedsgovernance skal implementeres, så det sikres, at roller, ansvar og kompetencer etableres på relevante niveauer i koncernen.
   - Styrelses- og myndighedschefer sætter koordinerede mål for informations-sikkerheden.
   - Styrelser og myndigheders opgaveløsning på informationssikkerhedsområdet skal placeres hensigtsmæssigt og tilpasses koncernens it-governance, så samarbejde mellem interessenter kan fungere effektivt.
   - Myndighedernes egenkontrol skal styrkes.

4. **Prioriteringer i 2018-2020 angående visionen om at "Arbejde helhedsorienteret med risikostyring":**

   - Helhedsorienteret risikostyring omfatter såvel vertikale som horisontale afhængigheder. Når flere styrelser deler informationer, inddrages risici affødt af gensidige afhængigheder.
   - Informationssikkerheden skal styres på grundlag af vurdering af risici frem for på et fast defineret regelgrundlag.
   - Kravene til informationssikkerhed skal afbalanceres med brugervenlighed og ressourceforbrug.
   - Leverandørers ansvar for og bidrag til risikovurderinger og beredskab skal defineres og realiseres. Dette gælder også for underleverandører, deres underleverandører mv.
   - Informationssikkerhedskrav skal implementeres i leverandørkontrakter på grundlag af CFCS' vejledninger.

5. **Prioriteringer i 2018-2020 angående visionen om at "Være ambitiøs og praksissættende":**

   - Vi vil være blandt de bedste til informationssikkerhed i Danmark.
   - Direktiver, bestemmelser og vejledninger skal gennemarbejdes, så de kan anvendes bredt også uden for koncernen.
   - Vi følger CFCS' vejledninger.

4. Indsatsområder og igangværende initiativer

Ud over førnævnte visioner og prioriteringer er der også andre forhold, som sætter relevante rammer for de konkrete initiativer, der skal realiseres i strategiperioden.

Dette gælder ikke mindst en række indsatsområder og igangværende initiativer, som er beskrevet i det følgende.

4.1 Governancestruktur

Forsvarministeriet har i sit Direktiv for den Militære Sikkerhedstjeneste inden for Forsvarsministeriets område af 1. juni 2017 fastlagt, at det overordnede ansvar for informationssikkerhed er forankret ved Forsvarsministeriet.

Forsvarsministeriets informationssikkerheds-governance er det system af regler, praksis og processer, som informations-sikkerhed styres efter i Forsvarsministeriets koncern.

Forsvarsministeriets informationssikkerheds-governance er et supplement til Forsvarsministeriets it-governance, FMIDIR 380-1, og styringen på området skal:

- understøtte den fortsatte digitalisering af koncernen,
- sikre, at der sættes klare mål for informationssikkerheden, og at der løbende følges op med relevant ledelsesinformation,
- ske hurtigt og effektivt på alle organisatoriske niveauer,
- tilpasse sig den hastige udvikling i trusselsbilledet og sårbarheder i forsvarets elektroniske informationssystemer og netværk.

Der er igangsat en opdatering af strukturen for informationssikkerhedsgovernance med henblik på, at den tilpasses governancestrukturen på it-området som beskrevet i FMIDIR 380-01. Arbejdet er etableret i Koncernfælles Informations-sikkerhedsudvalg med nedsættelse af en arbejdsgruppe med deltagere fra alle styrelser.

4.2 Koncernfælles Informations-sikkerhedsudvalg

Koncernfælles Informationssikkerhedsudvalg har til formål at styre informationssikkerheden på koncernniveau. Det er målet, at udvalget løbende orienteres om aktuelle cybertrusler med henblik på at igangsætte aktiviteter, der styrker informationssikkerheden på koncernniveau. Koncernfælles Informationssikkerhedsudvalg indtager en central position i den samlede governancestruktur og sikrer, at der med alle styrelsers deltagelse i udvalget er fælles fokus, retning og mål for informationssikkerheden.

4.3 Måling af informations-sikkerhedstilstanden

Der er igangsat et projekt om udarbejdelse af terminologi til beskrivelse af informations-sikkerhedsmål og metode til måling af sikkerhedstilstanden i koncernen. Vi har et ønske om at kunne måle, om vores indsats på informationssikkerhedsområdet lever op til de mål, vi sætter os. En god sikkerhedstilstand er opnået, når indsatsen opfylder målsætningerne. For at kunne kommunikere de målsætninger, der er sat for informationssikkerheden på koncernniveau, må vi have et fælles sprog til at beskrive retning og mål for arbejdet, herunder for hvad der er et passende sikkerhedsniveau for vores organisation. Dernæst skal vi have en måde, hvormed vi kan måle, om vi går i den rigtige retning, og om vi når vores mål.

4.4 Initiativer i Forsvarsministeriets it-strategi 2018-2020

Vi er i koncernen ved at realisere initiativet i Forsvarsministeriets it-strategi 2016-2019 om at implementere standarden ISO/IEC 27001:2013 med det formål at styre og højne informations-sikkerheden.

It-strategien beskriver andre initiativer, der kan have indflydelse på det generelle informations-sikkerhedsniveau som f.eks. konsolideringsinitiativet om ”Omlægning af identitets- og rettighedsstyring for it-brugere”, samt det yderst relevante udviklingsinitiativ ”Udvikling af kapacitet til forsvar mod trusler på internettet”.

De informationssikkerhedsrelaterede initiativer skal blandt andet ses i sammenhæng med it-strategiens vision ”Vores informationssikkerhed afspejler vores risikovillighed”, samt it-strategiens styringsprincip om, at ”Vi tænker på informationssikkerheden fra start til slut”.

5. Handleplan

Koncernen har med afsæt i nærværende strategis visioner og prioriteringer udvalgt konkrete initiativer til gennemførelse i løbet af strategiperioden, der løber fra 1. januar 2018 til 31. december 2020.

I annekserne til nærværende strategi er samtlige initiativer beskrevet separat.

For overblikkets skyld er initiativerne oplistet i tabellen herunder med angivelse af de koordinerende og bidragende myndigheder knyttet til initiativerne.

Visioner	**Initiativer**	**Koordinerende myndighed**	**Bidragende myndigheder**
1. Sikre et effektivt cyberforsvar og –beredskab	1.1 Udarbejdelse af minimumskrav til myndighedernes beredskabskapacitet	CFCS	Alle
	1.2 Samordning af awareness-aktiviteter	CFCS	Alle
2. Beskytte internetvendte systemer mod cyberangreb	2.1 Opfølgning på reduktion af angrebsflade	CFCS	FMN, VFK, FMI samt alle andre
3. Styrke styring og ledelse af informationssikkerhed	3.1 Implementering af governancestruktur	FMN	Alle
	3.2 Etablering af informationssikkerhedsportal på intranettet	CFCS	FMI samt alle andre
	3.3 Styrkelse af egenkontrol	CFCS	Alle
4. Arbejde helhedsorienteret med risikostyring	4.1 Samordning af leverandørstyring	CFCS	FMI samt alle andre
5. Være ambitiøs og praksissættende	5.1 Målsætning for informationssikkerhed	CFCS	Alle

Hvor der under "Bidragende myndigheder" er anført **alle**, skal det betragtes som et tilbud om bidrag.

Hvor der herudover eksplicit er anført en **myndighed**, er denne en obligatorisk bidragyder.

Gennemførelse af initiativerne vil ikke kræve lovgivning.

Økonomien for samtlige initiativer vil være inden for de deltagende parters egen ramme.

6. Tiden efter Forsvarsministeriets informationssikkerhedsstrategi 2018-2020

Nærværende strategi udløber med udgangen af 2020 samtidig med Forsvarsministeriets it-strategi. Ved udformningen af strategi på informationssikkerhedsområdet for 2021 og fremefter vil Forsvarsministeriet samordne den med udarbejdelsen af den næste it-strategi samt relevante nationale og internationale tiltag, der måtte ske i perioden. Forsvarsminsteriet vil bl.a. overveje mulighederne for at

- undersøge, om strategien har haft en positiv effekt, og hvilke indsatsområder som har givet størst effekt,
- forankre test af informationssikkerhedsberedskab i koncernstrategien,
- koncentrere indsatsen i forhold til afvikling af legacy systemer.

INITIATIV 1.1: Udarbejdelse af minimumskrav til myndighedernes beredskabskapacitet

Koordinerende myndighed
Center for Cybersikkerhed.

Initiativets indhold
Indledningsvis bemærkes det, at nærværende initiativ skal samordnes med det igangværende governancearbejde i koncernarbejdsgruppen for denne opgave.

Der skal iværksættes en tværgående koncern-arbejdsgruppe under ledelse af CFCS med henblik på udarbejdelse af minimumskrav til myndighedernes beredskabskapacitet på informationssikkerhedsområdet.

Dette arbejde vil, mht. indhold og tidsplan, i stor udstrækning afhænge af udviklingen af CFCS' 24/7 cybersituationscenter.

Minimumskravene skal afspejle myndighedernes forskellighed.

CFCS vurderer løbende, hvornår et kommissorium og en konkret arbejdsplan kan annonceres. Koncernen holdes orienteret kvartalsvist herom.

Baggrund
For at sikre et bredt løft i hele koncernen skal der udarbejdes minimumskrav til beredskabskapacitet gældende for samtlige myndigheder. Dette skal sikre et effektivt samspil mellem centrale og decentrale beredskaber på tværs af hele koncernen og derigennem styrke beredskabet.

Målgruppe
Samtlige myndigheder.

Effektmål
Som en del af initiativet skal der udarbejdes metrikker for måling af beredskabets effektivitet både under øvelser og skarpe situationer.

Organisering
Der er delvis angivet organisering under "Initiativets indhold". Udestående spørgsmål om organisering afklares af FMN.

Tidsplan
Initiativet løber fra det tidspunkt, CFCS igangsætter initiativet og frem til udgangen af 2019. Minimumskrav skal være endeligt udarbejdede og godkendt senest ved udgangen af 2019.

INITIATIV 1.2: Samordning af awareness-aktiviteter

Koordinerende myndighed
Center for Cybersikkerhed.

Initiativets indhold
Der skal iværksættes en generel samordning af koncernens arbejde med bruger-awareness om informationssikkerhed på grundlag af det vedtagne *Koncept for koordination og opfølgning på awareness vedrørende informationssikkerhed i Forsvarsministeriets koncern*.

Målet er at samle vejledninger og rådgivning om bruger-awareness i koncernen på den fælles informationssikkerhedsportal (Se initiativ 2.2), således at koncernfælles mål og temaer for awareness-aktiviteter baseret på det aktuelle trusselsbillede kan tilgås af myndighederne ét sted.

På den baggrund etableres:

- Fælles awareness-bibliotek for koncernens myndigheder på informationssikkerhedsportalen.
- Central udmelding af temaer for årets awareness-aktiviteter i lokale ISMS.

Fælles awareness-bibliotek
CFCS skal sammen med myndighederne og den primære it-leverandør i koncernen udarbejde et awareness-bibliotek om awareness for brugere på området for informationssikkerhed på den koncernfælles informationssikkerhedsportal på intranettet.

Portalen skal indeholde generelle vejledninger om awarenes-arbejdet ved myndighederne, vejledninger til brugerne om sikker adfærd til beskyttelse af koncernens informationer, rådgivning til myndigheder om etablering af lokale awareness-programmer og udformning af lokale informationssikkerhedsinstrukser til brugerne.

Central udmelding af temaer for årets awareness-aktiviteter i lokale ISMS
CFCS skal i samarbejde med Koncernfælles Informationssikkerhedsudvalg årligt – samt ad hoc efter behov – fastlægge overordnede mål eller temaer for koncernens awareness-aktiviteter i lyset af det aktuelle trusselsbillede.

I tillæg til dette skal informationssikkerhedsportalen støtte myndighedernes arbejde med de målrettede, koncernudmeldte awareness-aktiviteter gennem et katalog af tilgængelige ressourcer på området i koncernen – f.eks. information om relevante kurser, mulighed for bestilling af penetrationstests mv., gennemførelse af øvelser og evt. bistand hertil, gode råd og videndeling om erfaringer myndighederne imellem.

Baggrund
MIL.DK-sagen tydeliggjorde, at en af de største trusler for koncernen fortsat er brugeradfærd.

Bevidstheden om sikker adfærd på informations-sikkerhedsområdet skal højnes, og myndighederne i koncernen skal gennem målrettede aktiviteter sikre, at brugerne har den fornødne viden til at agere hensigtsmæssigt over for trusler mod informationssikkerheden.

Som led i koncernens ISO-arbejde er awareness et vigtigt indsatsområde, som bør gives central støtte og retning med bistand fra CFCS og den koncernfælles it-leverandør.

Der er forinden strategiperioden udarbejdet et awareness-koncept i koncernen.

Målgruppe
Samtlige myndigheder.

Effektmål
Nogle awareness-aktiviteter er uegnede til effekt-måling, mens andre er oplagte at måle på – f.eks. awarenessniveauet før og efter en awareness-kampagne rettet mod hele medarbejderstaben. Som et led i tilrettelæggelsen af en awareness-kampagne skal det overvejes, om der er behov og mulighed for, at en awareness-kampagne efterfølges af en test samt ledelsesopfølgning.

Ved at facilitere fælles målsætninger og temaer for aktiviteter i lyset af trusselsbilledet samt synliggøre

ressourcer og rådgivning på området for alle koncernmyndighederne, sikres det, at initiativet bidrager til en generel reduktion af it-risici forbundet med de koncernfælles it-systemer.

Organisering
Der er delvis angivet organisering under "Initiativets indhold". Udestående spørgsmål om organisering afklares af FMN.

Tidsplan
Initiativet skal være afsluttet ultimo 2019.

INITIATIV 2.1: Opfølgning på reduktion af angrebsflade

Koordinerende myndighed
Center for Cybersikkerhed.

Initiativets indhold
Der skal nedsættes en midlertidig arbejdsgruppe i koncernen. Som minimum vil den bestå af FMN, CFCS, VFK og FMI.

I løbet af en periode på tre måneder skal arbejdsgruppen analysere igangværende konkrete initiativer til reduktion af angrebsfladen mod internetvendte systemer.

I lyset af koncernens ambition om at vi vil være blandt de bedste til informationssikkerhed i Danmark, skal arbejdsgruppen vurdere og tage stilling til, hvad vi kan gøre i form af selvstændige initiativer til reduktion af angrebsfladen for koncernen.

Ved en eventuel beslutning og plan for nye initiativer på baggrund af ovenstående skal disse implementeres skridtvist i en hensigtsmæssig rækkefølge inden for den resterende del af strategiperioden.

Baggrund
De koncernfælles it-systemer, som er sikkerheds-godkendt til behandling af klassificeret information, driftes på interne netværk, der er sikret mod uautoriseret adgang. Derimod har cyberangreb mod koncernfælles internetvendte systemer i en række tilfælde været succesfulde, og det har været muligt for uautoriserede aktører at skaffe sig adgang til ansattes informationer af tjenstlig og privat karakter. Selvom disse informationer ikke er klassificerede, kan der være informationer, som koncernen ikke ønsker at offentliggøre. Der er derfor behov for at beskytte de mange adgange til og fra internettet ved at reducere angrebsfladen, herunder f.eks. ved at reducere antallet af koncernens mange internetadgange.

Målgruppe
Samtlige myndigheder.

Effektmål
Såfremt nye initiativer besluttes jf. afsnittet om initiativets indhold, skal effektmål beskrives individuelt for disse initiativer.

Organisering
CFCS er koordinerende myndighed for dette initiativ. Udestående spørgsmål om organisering afklares af FMN.

Tidsplan
Indledningsvis vil der være en analyseperiode på tre måneder. Ved en eventuel beslutning om nye initiativer på baggrund af analysen vil implementeringen heraf skulle foregå med afslutning ultimo 2019.

INITIATIV 3.1: Implementering af governancestruktur

Koordinerende myndighed
Forsvarsministeriet.

Initiativets indhold
Der er forinden strategiperioden nedsat en midlertidig governancearbejdsgruppe i koncernen.

Hovedformålet med nærværende initiativ 2.1 er at sikre en strategisk forankring og udførelse af den nødvendige implementeringsopgave, der skal igangsættes, når de fornødne krav til governance-struktur er defineret af koncernarbejdsgruppen.

I forbindelse med implementeringen skal to overordnede principper om forankring og samarbejde følges:

Roller, ansvar, kompetence og opgaveløsning skal forankres ved de relevante og hensigtsmæssige ledelsesniveauer.

Beslutninger om informationssikkerhed skal gennemføres og implementeres hurtigt og effektivt. Governance-strukturen skal derfor implementeres således, at samarbejdet mellem myndighederne er tæt, og at der er veldefinerede og hensigtsmæssige snitflader mellem forretningsansvarlige, forretningsrepræsentanter og it-ansvarlige i it-serviceudvalgene.

Baggrund
Forsvarsministeriets koncern er en stor organisation, sammensat af vidt forskellige myndigheder og, med en række indbyrdes afhængigheder inden for informationssikkerhed. En implementeret governancestruktur er derfor af vital betydning for koncernen.

Målgruppe
Samtlige myndigheder.

Effektmål
Initiativet er overvejende procesorienteret, hvilket umiddelbart begrænser den direkte effekt-målbarhed. Ved at sikre en hensigtsmæssig implementering af governancestruktur på området for alle koncernmyndighederne sikres det, at initiativet bidrager til en generel reduktion af it-risici forbundet med de koncernfælles it-systemer.

Organisering
Udestående spørgsmål om organisering afklares af FMN.

Tidsplan
Initiativet skal være afsluttet ultimo 2019.

INITIATIV 3.2: Etablering af informationssikkerhedsportal på intranettet

Koordinerende myndighed
Center for Cybersikkerhed.

Initiativets indhold
CFCS skal sammen med forretningen og den primære it-leverandør i koncernen etablere en koncernfælles informationssikkerhedsportal på intranettet under hensyntagen til samordning af eksisterende portalfunktioner, hvor det er relevant. Portalen skal støtte myndighedernes arbejde med informationssikkerhed bl.a. gennem et katalog af tilgængelige services og ressourcer på området i koncernen, herunder information om:

- vejledninger og skabeloner
- forvaltningsgrundlag
- vejledning til underretning om sikkerhedsbrud samt overblik
- KPI'er på performance, uddannelse osv.
- relevante kurser
- mulighed for rådgivning
- mulighed for bestilling af penetrationstests mv.
- leverandørers anvendelse/tilslutning til Netsikkerhedstjenesten
- leverandørers anvendelse af branchestandarder
- gennemførelse af øvelser og evt. bistand hertil
- gode råd og videndeling om erfaringer myndighederne imellem om awareness for brugere på informationssikkerhedsområdet

I takt med koncernens opbygning af et stærkere, samlet cyber- og informationsssikkerhedsberedskab, vil det være naturligt at anvende en separat del af portalen til et beredskabskatalog, herunder med beredskabsrelateret information om myndighedernes:

- status for implementering af minimumskrav til beredskab
- planer
- organisation
- kontaktlister
- øvelsesaktiviteter.

Baggrund
Der er et ønske fra myndighederne om at vide, hvor man skal henvende sig for at få hjælp til informationssikkerhedsarbejdet. Der er behov for et fælles sted at slå op, for at få overblik over ressourcer, tjenester og ekspertiser inden for koncernen generelt samt specifikt for it-sikkerhedsmyndigheden, CFCS.

Målgruppe
Samtlige ansatte i koncernen.

Effektmål
Initiativet er overvejende procesorienteret, hvilket umiddelbart begrænser den direkte effektmålbarhed. Ved at synliggøre ressourcer og rådgivning på området for alle koncernmyndighederne vil initiativet kunne bidrage til en generel reduktion af it-risici forbundet med de koncernfælles it-systemer.

Organisering
Der er delvist angivet organisering under "Initiativets indhold". Udestående spørgsmål om organisering afklares af FMN.

Tidsplan
Initiativet skal være afsluttet ultimo 2019.

INITIATIV 3.3: Styrkelse af egen-kontrol

Koordinerende myndighed
Center for Cybersikkerhed.

Initiativets indhold
Myndighedernes egenkontrol skal styrkes.

CFCS skal rådgive og støtte myndighederne i disses bestræbelser, herunder en hensigtsmæssig planlægning og tilrettelæggelse af egenkontrollen.

Samtlige myndigheder fortsætter det daglige arbejde med egenkontrol samtidig med, at:

- CFCS og FMN i første halvår af 2018 gennemfører en analyse af, hvordan de oven for nævnte mål kan opnås,
- resultatet af analysen implementeres i resten af strategiperioden.

Disse opgaver udføres i dialog med myndighederne.

Baggrund
Tilsynet med informationssikkerheden udgør et vigtigt element i governance for informations-sikkerheden.

På vegne af departementet og som it-sikkerheds-myndighed fører Center for Cybersikkerhed tilsyn med informationssikkerheden i koncernen. Departementet fører tilsyn med, at centerets tilsyn udføres tilstrækkeligt og effektivt.

Tilsynet med informationssikkerheden gennemføres med det formål at vurdere, om informations-sikkerheden ved styrelser og øvrige myndigheder i koncernen er tilrettelagt således, at informationers tilgængelighed, fortrolighed og integritet sikres i overensstemmelse med bestemmelsesgrundlaget og de fastsatte mål for informationssikkerheden.

It-sikkerhedsmyndighedens årlige tilsyn vil fortsat have fokus på koncernstyrelsernes styring af informationssikkerheden ved egen og underlagte myndigheder. Tilsynet vil dog i strategiperioden gradvist bevæge sig mod flere udvidede tilsyn ved udvalgte myndigheder og med udvalgte temaer ud fra kriterierne risiko og væsentlighed.

Koncernens styrelser og øvrige myndigheder prioriterer - som minimum årligt - at gennemføre egenkontrol af informationssikkerheden inden for eget myndighedsområde i henhold til gældende bestemmelsesgrundlag. Ud af den samlede mængde tilsynsaktiviteter i koncernen udgøres størstedelen således af egenkontrol lokalt hos myndighederne.

I forbindelse med denne store opgave har myndighederne behov for rådgivning og støtte til at tilrettelægge deres egenkontrol hensigtsmæssigt.

Målsætning
Minimumsmålsætninger fremgår under "Initiativets indhold".

Målgruppe
Samtlige myndigheder.

Effektmål
Initiativet er overvejende procesorienteret, hvilket umiddelbart begrænser den direkte effekt-målbarhed. Ved at sikre en hensigtsmæssig egenkontrol på området for alle koncern-myndighederne, sikres det, at initiativet bidrager til en generel reduktion af it-risici forbundet med koncernens it-systemer. Der vil imidlertid kunne måles kvantitativt på mængden af egenkontrol, der er gennemført af myndighederne.

Organisering
CFCS er koordinerende myndighed for dette initiativ. Udestående spørgsmål om organisering afklares af FMN.

Tidsplan
Initiativet skal være afsluttet ultimo 2019. I 1. halvdel af 2018 gennemføres analysedelen. Resultatet heraf implementeres indtil udgangen af 2019.

INITIATIV 4.1: Samordning af leverandørstyring

Koordinerende myndighed
Center for Cybersikkerhed.

Initiativets indhold
Der iværksættes en samordning af koncernens arbejde med leverandørstyring i forhold til it-services, herunder it-produkter, -systemer og -drift. Dette sker både i forhold til interne og eksterne leverandører. Der skal især være fokus på følgende områder:

- Fastlæggelse af gensidige informations-sikkerhedsforpligtelser i kontrakter – dvs. både for leverandørerne og forretningen.
- Indhentning og audit af relevant information fra leverandører for bl.a. at sikre leverandørernes efterlevelse af ISO 27000-serien, hvor det er relevant, og andre branchestandarder.
- Erkendelse af risikobilledet og kontinuerlig stillingtagen til dets udvikling i takt med ændrede trusler, sårbarheder, sandsynligheder, modforanstaltninger mv. Denne stillingtagen skal tillige omfatte inddragelse af risici affødt af gensidige afhængigheder på tværs af koncernen, dvs. både i forhold til side-, over- og underordnede myndigheder samt leverandører.

For hvert af disse tre punkter er der på forhånd opstillet følgende målsætninger:

- **Fastlæggelse af gensidige informationssikkerhedsforpligtelser i kontrakter**
  CFCS skal sammen med forretningen og den primære it-leverandør i koncernen udarbejde en vejledning til fastlæggelse af kontraktlige forpligtelser om informationssikkerhed og dokumentation på området. For interne leverancer i koncernen skal der som udgangspunkt fastlægges forpligtelser om informationssikkerhed svarende til leverancer fra eksterne leverandører.
- **Indhentning og audit af relevant information fra leverandører**
  CFCS skal sammen med forretningen og den primære it-leverandør i koncernen udarbejde en vejledning til indhentning og audit af relevant information fra leverandører.
- **Erkendelse af risikobilledet og kontinuerlig stillingtagen til dets udvikling**
  For at forretningen bedre kan forstå og afspejle risici fra leverandørlaget i vurderingen af informationssikkerhedsrisici, skal FMI etablere og vedligeholde et fælles dokumentationsbillede gældende for koncernfælles it-systemer leveret af FMI.

I dokumentationsbilledet skal der tillige indgå andre it-systemer, der har eget it-serviceudvalg. Det er leverandørerne af disse it-systemer, der leverer væsentlige indholdsdele til dokumentationsbilledet for de pågældende systemer.

Dokumentationsbilledet kan for eksempel bestå af servicedeklarationer og bør som minimum omfatte sårbarhedsvurderinger og opdateret dokumentation for implementering af kontroller (VFKBST 358-1 / ISO 27001 Annex A kontroller).

Hvor det er relevant, bør information om implementering af kontroller på baggrund af CFCS' vejledninger og trusselsvurderinger tillige indarbejdes i dokumentationsbilledet.

Det er tanken, at forretningen skal kunne kombinere leverandørlagets systemrisici med de risici, som forretningen identificerer i relation til forvaltning og anvendelse af systemerne.

Det skal overvejes, hvorledes dokumentation for risikostyringen i koncernfælles it-systemer stilles til rådighed for myndighedernes egen risikostyring, herunder muligheder for at dette sker gennem it-baserede værktøjer.

Baggrund
Koncernen har i de seneste år oplevet en stigende kompleksitet i arbejdet med leverandørstyring, som bl.a. skyldes øget diversitet i systemporteføljer, -

platforme og -processer samt øget kompleksitet af værdikæder, trusselsbilleder, risikomitigering mv.

Målgruppe
Samtlige myndigheder.

Effektmål
Ved at facilitere en samordning af arbejdet med leverandørstyring, resulterende i højnet kvalitet af dette arbejde, må det forventes, at initiativet bidrager til en generel reduktion af risici forbundet til de koncernfælles IT-systemer.

Det skal som minimum kunne måles, hvorvidt der er implementeret og dokumenteret kontroller / foreligger opdaterede servicedeklarationer, samt hvorvidt der er stillet oplysninger til rådighed om sårbarheder/modforanstaltninger mv. for koncernen.

Organisering
Der er delvist angivet organisering under "Initiativets indhold". Udestående spørgsmål om organisering afklares af FMN.

Tidsplan
Initiativet skal være afsluttet ultimo 2019.

INITIATIV 5.1: Målsætning for informationssikkerhed

Koordinerende myndighed
Center for cybersikkerhed.

Initiativets indhold
Med afsæt i ISO/IEC 27001 skal myndighederne sætte mål for informationssikkerhedsarbejdet, og muligheden for at måle, om målsætninger er nået, skal forbedres.

Der skal udvikles følgende:

1. Et metodeapparat til at fastlægge, hvad et passende informationssikkerhedsniveau for en organisation er.

2. En terminologi til at beskrive det ønskede informationssikkerhedsniveau eller målsætning for informationssikkerhed.

3. Metode til at måle hvor langt man er fra at opfylde målene som et udtryk for sikkerhedstilstanden.

Baggrund
Myndigheder i Forsvarsministeriets koncern har i stigende grad behov for at betrygge sig selv og eksterne interessenter i, at deres indsats i forhold til informationssikkerhed bibringer dem et passende sikkerhedsniveau. Derfor er der et behov for at udvikle en model for, hvordan man kan måle sikkerhedstilstanden ved en given myndighed samt sammenligne resultaterne på tværs i organisationen.

Målgruppe
It-sikkerhedschefer og sikkerhedsofficer ved alle myndigheder i koncernen.

Effektmål
De forventede gevinster ved at gennemføre initiativet er, at forsvaret dels vil kunne vurdere, om informationssikkerhedsindsatsen er tilstrækkelig, dels at kunne vurdere, om det anvendte ressource-forbrug er passende. Dette giver mulighed for, at potentialer i ressourceoptimering kan identificeres og realiseres.

Organisering
CFCS udarbejder udkast til metoder og terminologi som pilottestets. Denne opgave færdigbearbejdes i samarbejde med én myndighed.

Tidsplan
Initiativet løber i hele 2018, således at udkast til metoder udvikles i første kvartal, pilot gennemføres i andet og tredje kvartal, og metoderne udrulles i resten af koncernen i fjerde kvartel.