Sikkerhedskrav og sikkerhedsydelser på SKI's aftaler

Software Summit 2025

November 2025

Peter Godiksen, Chefkonsulent

Indhold

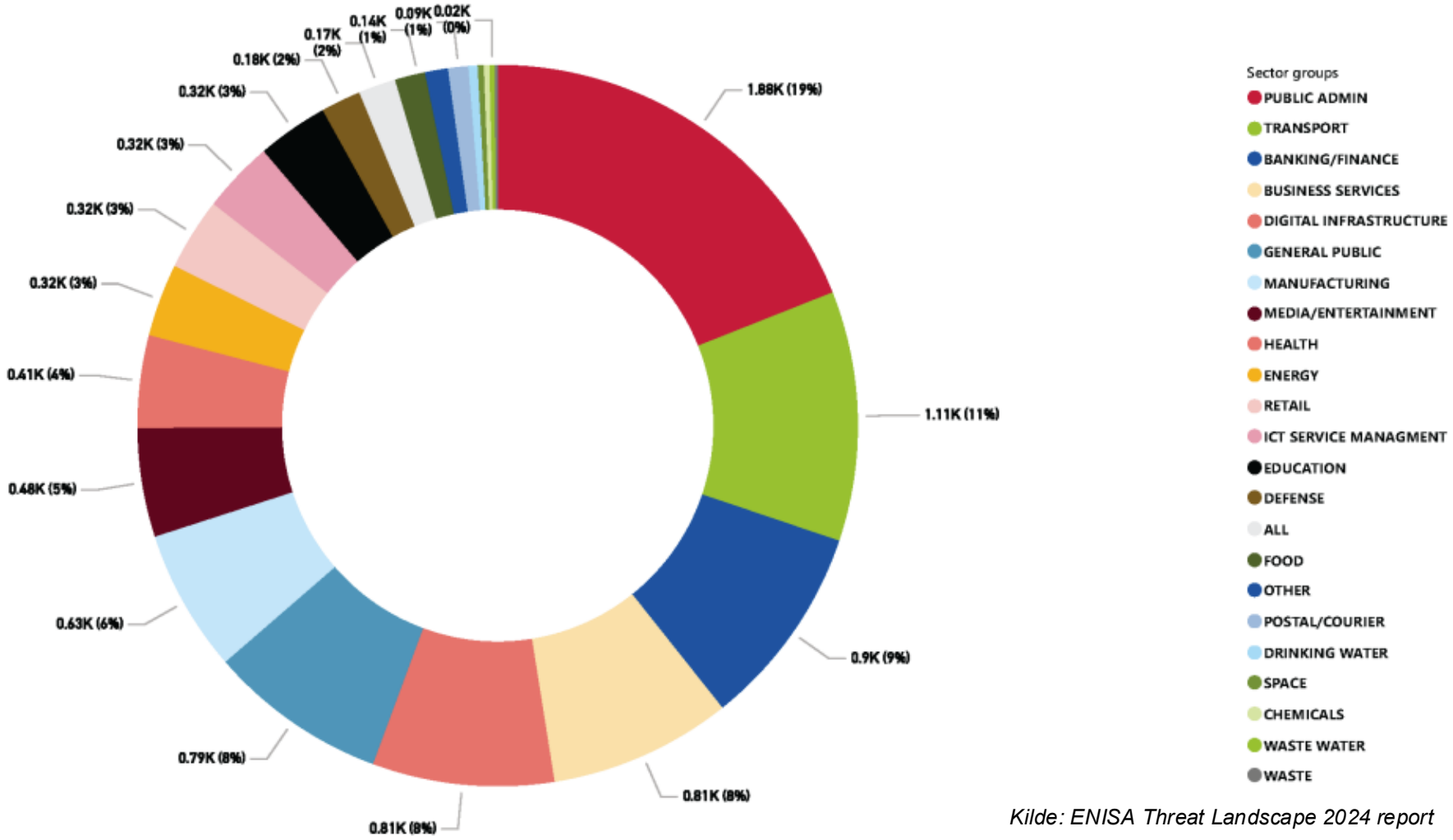
- Sikkerhed i indkøb skal beskytte individ, organisation og samfundet
- Informationssikkerhed på SKIs' it- aftaler
- Eksempler på krav til informationssikkerhed på SKI's it-konsulentaftaler, softwareaftaler og teleaftaler

SKI

Sikkerhed i indkøb skal beskytte individ, organisation og samfundet

Den offentlige sektor er mest udsat for angreb

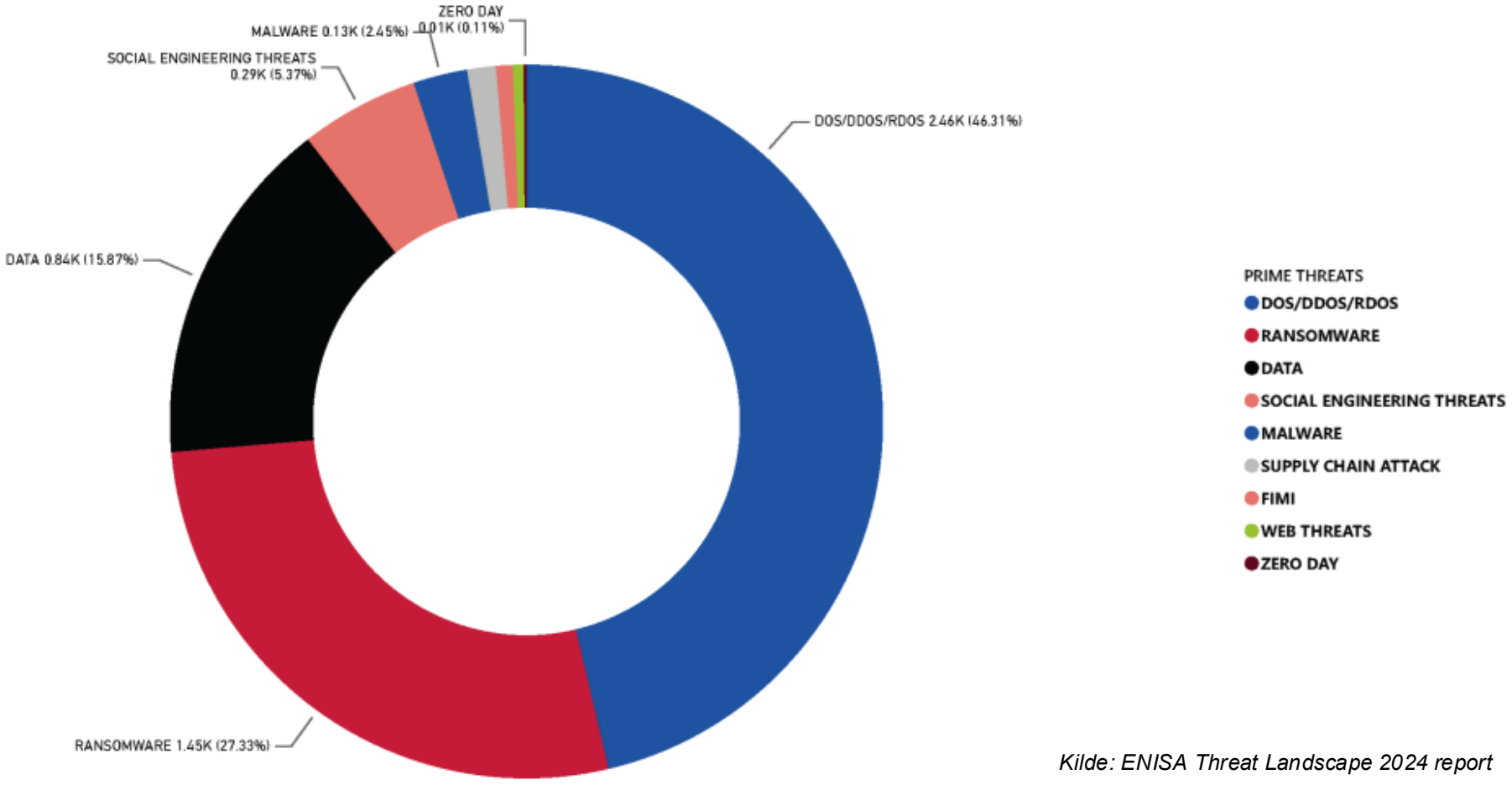
Figure 6 Targeted sectors per number of incidents (July 2023 - June 2024)



Kilde: ENISA Threat Landscape 2024 report

Hvilke angreb udsættes den offentlige sektor for?

Figure 5: EU breakdown of number of threats by threat group



Kilde: ENISA Threat Landscape 2024 report

NIS2-direktivet skal styrke den samfundsmæssige sikkerhed

Hvad er NIS2?

- NIS2 er den almindelige betegnelse for EU-direktiv (EU) 2022/2555, som fastlægger foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i EU
- NIS2-direktivet bygger ovenpå og ophæver EU-direktivet om sikkerhed i net- og informationssystemer (NIS1-direktivet)
- **EU-direktivet er udmøntet i national lov og trådte i kraft den 1. juli 2025.** Herefter skal de virksomheder og myndigheder, der er omfattet, efterleve kravene i lovgivningen samt eventuelle yderligere krav, som er fastsat i EU-regi eller i bekendtgørelser.

Hvad er formålet?

- Forbedre cybersikkerheden på tværs af EU
- Styrke modstandsdygtigheden mod cyberangreb
- Skabe ensartede krav til virksomheder og organisationer
- Øge samarbejdet mellem EU's medlemslande i tilfælde af cybertrusler.

Krav

- **Risikostyring:** Virksomheder skal foretage risikovurderinger og implementere passende sikkerhedsforanstaltninger
- **Hændelsesrapportering**: Cybersikkerhedshændelser skal rapporteres til myndighederne inden for 24 timer
- **Forretningskontinuitet**: Virksomheder skal have en beredskabsplan for at kunne opretholde drift under cyberangreb
- **Ledelsesansvar**: Bestyrelser og ledelser får et direkte ansvar for at sikre overholdelse af NIS2.

Kilde: NIS2-loven

SKI

De 10 sikringsforanstaltningsområder fra NIS2-loven

Foranstaltninger til styring af cybersikkerhedsrisici

§ 6. Væsentlige og vigtige enheder skal træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester. Foranstaltningerne skal som minimum omfatte følgende:

1) Politikker for risikoanalyse og informationssystemsikkerhed.

2) Håndtering af hændelser.

3) Driftskontinuitet, herunder backupstyring og reetablering efter en katastrofe og krisestyring.

4) Forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere.

5) Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder.

6) Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici.

7) Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse.

8) Politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering.

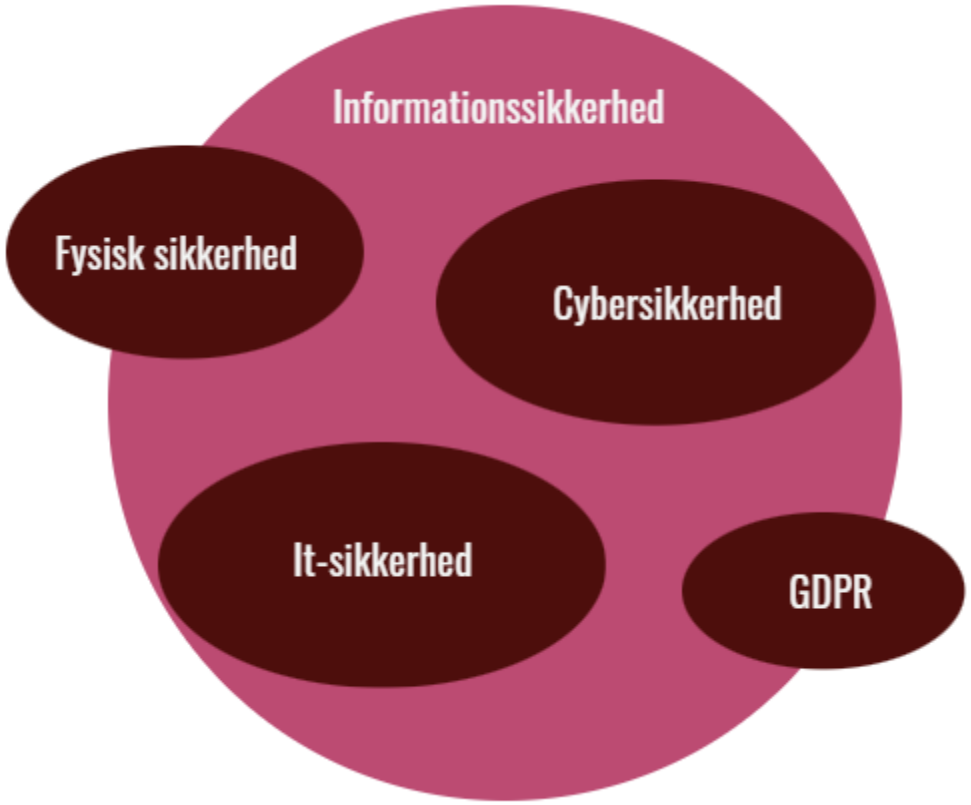
9) Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver.

10) Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt hos enheden, hvor det er relevant.

SKI

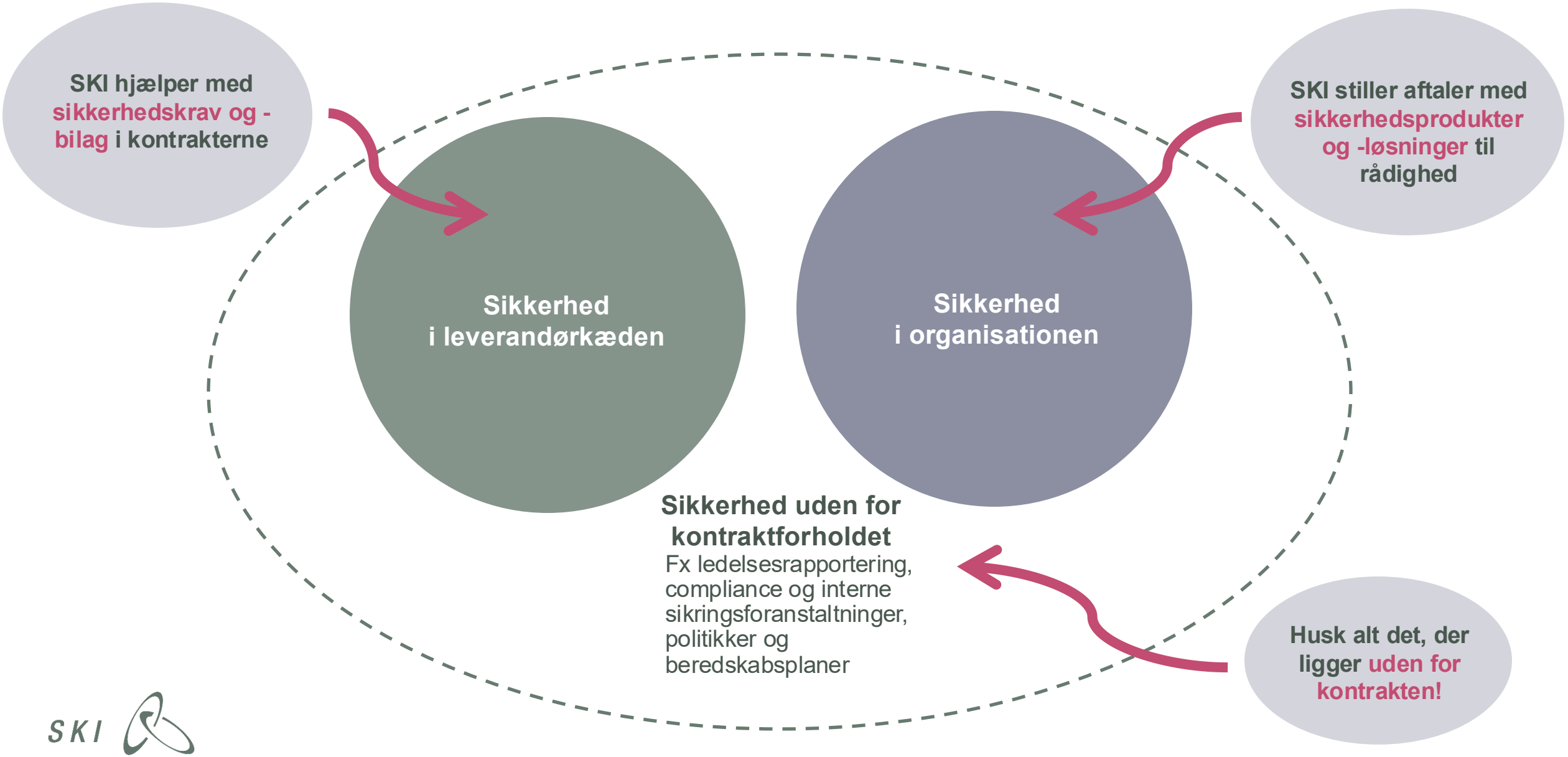
SKI ser helhedsorienteret på informationssikkerhed

- **Informationssikkerhed** omfatter alle typer af information – både fysisk og digitalt – såsom persondata og forretningsdata.
- **It-sikkerhed** beskytter information, der behandles i it-systemer (hardware og software) mod uautoriseret adgang, brug eller ændring.
- **Cybersikkerhed** dækker over it-sikkerhed for netværksforbundne systemer og beskyttelse mod angreb via netværk eller internettet.
- **Fysisk sikkerhed** beskytter data, udstyr og mennesker, der befinder sig på fysiske lokationer, mod uautoriseret adgang og skader.
- **GDPR** er specifikt rettet mod beskyttelse af persondata og sikring af borgernes rettigheder. Selvom GDPR og informationssikkerhed ofte nævnes sammen, dækker GDPR også områder, der ligger ud over det, man normalt forbinder med informationssikkerhed, som fx ret til indsigt i egne data og til at blive ”glemt”.



Informationssikkerhed på SKI's it-aftaler

Informationssikkerhed: Hvor kan SKI hjælpe?



Sikkerhed i SKI-aftaler – hvad gør SKI?

Vi kategoriserer aftaler ud fra fire niveauer/kategorier:

- Kontraktens genstand/opgaven
- Kritikalitet af potentiel forretningsunderstøttelse
- Dataflow og -adgang
- Regulatoriske krav – NIS2, CRA, AIA mv.

Vi udarbejder krav til sikkerhed på aftalerne

- Kontraktens genstand/opgaven
- Pakker og niveauer.

Leverandører på SKI-aftaler er en blanding af direkte og indirekte omfattede virksomheder → forskellig modenhed.

Eksempler på aftalers placering i kategorier for kritikalitet

Gruppe 1
50.30 Møbler, 50.04 Tidsskrifter
50.55 Kontorartikler

Gruppe 4
02.19 Fagsystemer, 02.17 It-konsulenter, 02.22 It-drift

SKI hjælper med at løfte dit ansvar for informationssikkerhed

SKI's sikkerhedskrav er tilpasset lovgivning og risikoprofil

- Mange af SKI's aftaler indeholder relevante sikkerhedskrav, der tager højde for lovgivningsmæssige tiltag, herunder GDPR og NIS2.
- SKI foretager risikovurderinger på tværs af leverancetyper (fx software, konsulentydelser, infrastruktur) og tilpasser kravene til risikoprofilen på den enkelte aftale.

Vi hjælper med at omsætte behov til de rette krav

- SKI hjælper med at omsætte sikkerhedsbehov til løsninger.
- Få vejledning i at vurdere din organisations sikkerhedsbehov og stille de rigtige krav.
- Få input til risikovurdering, kravspecifikation og markedsdialog.

Få let adgang til bredt udvalg af sikkerhedsløsninger

- Hurtig adgang til sikkerhedsløsninger, fx software og licenser, rådgivning og konsulentydelser og managed services.

Informationssikkerhed i leverandørkæden: Sikkerhedsbilag i kontrakterne

Aftalens kritikalitet

Hvor vigtig er aftalen for drift og sikkerhed?

Datas fortrolighed

Hvilke data kan leverandøren kan få adgang til – og hvor følsomme er de?

Leverandørens adgang

Hvordan og hvor får leverandøren adgang til data?

Sikkerhedskrav fastsættes for hver enkelt aftale

SKI

Sikkerhed i offentlige indkøb

Hvilket produkt, ydelse, tjeneste mv. købes?

- It-produkter, IoT, software
- Større it-løsninger
- Juridiske tjenesteydelser
- Forskning og udvikling
- Outsourcing af it-drift
- Bygningsservice
- Logistik – transport, lager distribution

Hvilken type data kan potentielt blive delt med leverandøren eller eksponeret via ydelsen?

- Forretningskritisk data
- Juridiske data
- Logistiske data
- Ledelsesinformation
- IP
- Almindelige eller følsomme persondata

Hvilken adgang vil leverandøren have til kundens data og informationssystemer

- Cloud hos leverandøren
- Fysisk adgang
- Fjernadgang
- Underleverandører
- Type af miljø

Vurdering pr kontrakt:
Er NIS2 relevant? Hvilke krav til sikkerhed skal der indarbejdes?

SKI

Sådan understøtter it-aftalerne NIS2 og krav til informationssikkerhed

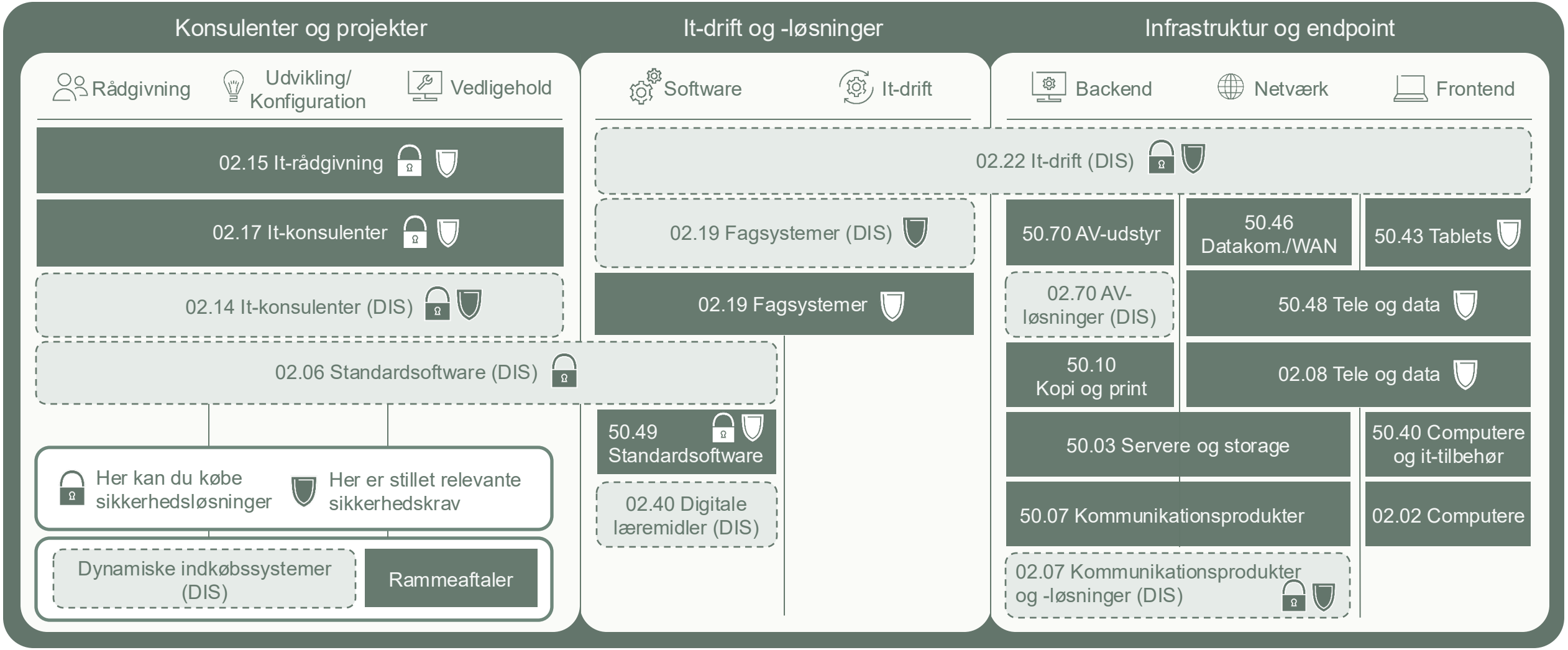
SKI's fire bidrag

1. **Opdaterede sikkerhedskrav**
   - SKI arbejder systematisk på at opdatere sikkerhedskravene i vores aftaler i takt med genudbud og opdateringer, så de er i overensstemmelse med NIS2
2. **Sikkerhedsløsninger**
   - SKI stiller aftaler med sikkerhedsløsninger og -ydelser til rådighed, der kan købes ind på som led i at højne sikkerheden i din organisation
3. **Rådgivning og vejledning**
   - SKI tilbyder vejledning om sikkerhedskrav på aftalerne og sikkerhedsanskaffelser
4. **Samarbejde med sikkerhedsmyndigheder**
   - SKI samarbejder med relevante myndigheder som fx SAMSIK for at sikre, at krav og vejledninger baseres på det aktuelle risikobillede

SKI stiller krav til produkter og ydelser

- **SKI stiller krav til leverandørerne om:**
  - Tekniske og organisatoriske sikkerhedsforanstaltninger (herunder adgangsstyring, hændelseshåndtering og dataintegritet)
  - Leverandørens dokumentation og egenkontrol
  - Leverandørens håndtering af underleverandører
  - Opfyldelse af relevante internationale standarder, herunder ISF's Standard of Good Practice for Information Security, ISO 27002, CIS18 og NIST Cybersecurity Framework
- **SKI har desuden indført krav om revisionserklæringer** i flere rammeaftaler for at sikre leverandørernes overholdelse af sikkerhedskravene

Overblik over sikkerhedskrav og –løsninger på SKI's it-aftaler



SKI's it-aftaler med sikkerhedsprodukter og -ydelser

- De fleste af de produkter og ydelser, det offentlige har behov for i forbindelse med NIS2 og sikkerhed generelt, er tilgængeligt via SKI's aftaler.
- Det omfatter bl.a. tekniske sikkerhedsløsninger som fx SIEM, end point detection, adgangskontrol, net-værksovervågning.
- Du kan også købe strategisk eller praktisk rådgivning til at komme godt i mål med din sikkerhedsindsats inden for bl.a. cybersikkerhedsstrategi og -governance, trusselsmodellering og risikoscenarier, incident response og beredskabsplaner, awareness og organisatorisk forankring og overholdelse af lovgivning, herunder NIS2 og ISO 27001.

OVERBLIK OVER SIKKERHEDSYDELSER PÅ SKI-AFTALER

02.06 Standardsoftware	02.07 Kommunikations-produkter og -løsninger	02.14 It-konsulenter 02.15 It-rådgivning 02.17 It-konsulenter	02.22 It-drift
Ydelsesområde: **Sikkerhed**	Ydelsesområde: **It-sikkerhedsprodukter ***	Ydelsesområde: **It-sikkerhed, business continuity & it-compliance**	Ydelsesområde: **Sikkerhedsservices**
Integrated Risk Management	DDOS (Distributed Denial Of Services)	Etablering af it-sikkerhed	IAM (Identity & Access Management)
Consumer Security Software	SIEM & SOC	Kriseledelse, business continuity og disaster recovery	SIEM (Security Information & Event Management)
Endpoint Protection Platforms (Enterprise)	Endpoint protection	IT-compliance	SOC (Security Operations Centre)
Secure Email Gateways	IDPS (Intrusion Detection & Prevention System)		
Security Information and Event Management Software	Firewalls		
Secure Web Gateways	Management af it-sikkerhedsprodukter		
Threat Intelligence			
Identity Governance and Administration			
Application Security Testing			
Vulnerability Assessment			
Web Application Firewall			
Access Management			
Privileged Access Management			
User Authentication			
Enterprise Data Loss Prevention			
Encryption			
Tokenization			
Cloud Access Security Brokers			

Eksempler på krav til informationssikkerhed på SKI's it-konsulentaftaler, softwareaftaler og teleaftaler

Sikkerhedskrav i SKI's it-konsulentaftaler – overvejelser og risici

Insider

Kollegaer

Arbejdsplads

Arbejdsredskaber

Arbejdssted

Cyberkriminalitet

Hybridkrig

Regulering:
GDPR, NIS2
AI Act, CER
Etc., etc., etc

Fortrolig information

Sensitive data

Viden

SKI

Sikkerhedskrav på 02.15 It-rådgivning og 02.17 It-konsulenter

Rammeaftalens punkt 11.4 Sikkerhed, sikkerhedsgodkendelse og persondata

- Vedrører krav til leverandøren
- Krav om overholdelse af ISO/IEC 27001 eller tilsvarende og krav i B.3
- Eventuelt sikkerhedsgodkendelse af konsulenter, hvis kunder kræver det
- It-sikkerhedsrevision (punkt 11.4.4) ift. kravene i bilag B.3 Sikkerhedskrav (ISAE 3000 type 1 og 2 revisionsrapport)

Rammeaftalens Bilag B.3 Sikkerhedskrav

- Vedrører kundens valg af kravpakke m.v. og leverandøren mht. efterlevelse af krav
- Krav er baseret på Security Forums (ISF) Standard of Good Practice (SGOP) og ISO 27002.)
- Leverandørerne bliver auditeret ift. implementering og efterlevelse af sikkerhedskravene. SKI foretager opfølning på dette.
- Sikkerhedskravene/-foranstaltninger er inddelt i pakker; B, 1, 2 og 3 samt en række tillægsforanstaltninger

Leveringskontraktens punkt 8.7 Sikkerhed, legitimation og persondata

- Vedrører leverancen og kontrakten mellem kunde og leverandør
- Leverandøren skal overholde kravene i Rammeaftalens punkt 11.4 og kravene til sikkerhed, jf. bilag B.3 Sikkerhedskrav
- Legitimation: Leverandørens medarbejdere eller samarbejdspartnere skal bære synligt billedidentifikationskort ifm. leverancer på Kundens adresser eller lokationer
- Persondata: Såfremt leverandøren behandler persondata på vegne af kunden er parterne forpligtet til at indgå en databehandleraftale, der overholder den seneste version af Datatilsynets Standardkontraktbestemmelser på tidspunktet for indgåelse af databehandleraftalen

Leveringskontraktens Bilag E.4 Databehandleraftale

- Vedrører leverancen og kontrakten mellem kunde og leverandør
- Såfremt leverandøren behandler persondata på vegne af kunden er parterne forpligtet til at indgå en databehandleraftale, der overholder den seneste version af Datatilsynets Standardkontraktbestemmelser på tidspunktet for indgåelse af databehandleraftalen
- Parterne kan ikke udfylde databehandleraftalen, jf. ovenfor, med vilkår, der ikke er i overensstemmelse med, eller på anden vis strider mod, vilkårene i Leveringskontrakt eller Leverandørens forpligtelser i henhold til Rammeaftalen
- Leverandøren må i så fald ikke påbegynde behandling af personoplysninger forinden, databehandleraftalen er indgået

Sikkerhedskrav på it-konsulentaftalerne 02.14, 02.15 og 02.17

- Aftalerne omfatter tillægsforanstaltninger med sikkerhedskrav.
- Tillægsforanstaltninger bliver aktiveret ved behov for:
  - **Fjernadgang**
  - **Mobile**
  - **BYOD**
  - **Udvikl**
  - **Projekt.**
- Kravene fremgår af rammeaftalens Bilag B.3 Sikkerhedskrav.

- **1 (Få):** Få almindelige personoplysninger, få forretningskritiske data samt adgang til ikke-kritiske systemer og applikationer.
- **2 (Nogle):** nogle (omfang vurderes af kunden) almindelige personoplysninger, nogle forretningskritiske data og adgang til enkelte kritiske systemer.
- **3 (Mange):** adgang til følsomme personoplysninger, mange almindelige personoplysninger, fortrolige data, mange forretningskritisk data samt flere kritiske systemer
- **B (Basis):** Hvis medarbejderen ikke skal have adgang til nogen former for følsomme/fortrolige eller kritiske data/systemer og medarbejderen alene arbejder hos kunden og med kundens udstyr.

Kritikalitet og mængde af information/adgang					
Typer af information/ adgang	Ingen (B)	Få (1)	Nogle (2)	Mange (3)	
Adgang til forretningskritiske systemer	Nej				Valg giver pakke B – 1 – 2 – 3 krav
Forretningskritisk information	Nej				Valg giver pakke B – 1 – 2 – 3 krav
Almindelige personoplysninger	Nej				Valg giver pakke B – 1 – 2 – 3 krav
Følsomme personoplysninger				Ja	Ved Ja – pakke 3 krav
Adgang til samfunds kritisk infrastruktur (systemer og data)				Ja	Ved Ja – pakke 3 krav

SKI

Sikkerhedskrav med tillægsforanstaltninger på It-konsulentaftalerne

- Aftalerne omfatter tillægsforanstaltninger med sikkerhedskrav.
- Tillægsforanstaltninger bliver aktiveret ved behov for:
  - **Fjernadgang**
  - **Mobile**
  - **BYOD**
  - **Udvikl**
  - **Projekt.**
- Kravene fremgår af rammeaftalens Bilag B.3 Sikkerhedskrav.

Tillægspakke	Relevant, hvis
Fjernadgang	Leverandørens medarbejdere arbejder på Leverandørens udstyr fra Leverandørens lokationer Leverandørens medarbejdere arbejder på Leverandørens udstyr hjemme fra
Mobile	Leverandørens medarbejdere arbejder på Leverandørens udstyr, dvs. Leverandørens bærbare PC'er, tablets og smartphones
BYOD (bring your own device)	Medarbejderen benytter eget udstyr, dvs. medarbejderens eget udstyr
Udvikl	Leverandøren skal rette/ændre/tilpasse kode eller konfigurationer i kritiske systemer og applikationer, jf. bilag E.1 Kundens opgavebeskrivelse
Projekt	Leverandøren har projektledelsesansvar jf. bilag E.1 Kundens opgavebeskrivelse

SKI

Krav til Type 1 og Type 2 revisionserklæringer på 02.15 It-rådgivning og 02.17 It-konsulenter

Fremsende Type 1 revisionserklæring til SKI

- I skal senest 3 måneder efter rammeaftalens ikrafttrædelsen, fremsende en ISAE 3000 Type 1 revisionserklæring til SKI.
- Revisionserklæringen skal være baseret på auditering af jeres samlede sikkerhedsimplementering af kravene i bilag B.3 i form af etablerede sikkerhedsprocedurer til SKI.

Årligt udfærdige Type 2 revisionserklæring

- I skal herefter årligt udfærdige en ISAE 3000 Type 2 revisionserklæring baseret på auditering af jeres samlede sikkerhedsimplementering af kravene i bilag B.3 i form af etablerede sikkerhedsprocedurer samt faktisk håndtering og efterlevelse heraf ved levering af ydelserne. Den skal sendes til SKI.
- SKI kan ved anmodning fra kunden udlevere den pågældende rapport til kunden under hensyntagen til gældende lovgivning.

Bod ved manglende erklæring

- Såfremt tidsfristen for fremsendes af ISAE 3000 revisionserklæringen ikke efterleves, vil der ifalde en dagbod på 3.000 kr. pr. påbegyndt arbejdsdag indtil det tidspunkt SKI har modtaget rapporten.
- Bodsbeløbet kan ikke overstige 100.000 kr. pr. tilfælde.

Påkrav om efterlevelse af sikkerhedskrav

- Såfremt revisionserklæringen viser, at leverandøren ikke efterlever kravene i bilag B.3, vil SKI sende et påkrav om at rette op på de pågældende forhold indenfor en given tidsfrist.
- Overholder leverandøren ikke dette indenfor den givne tidsfrist, ifalder der SKI en dagbod på 5.000 kr. pr. påbegyndt arbejdsdag fra fristens udløb.
- Bodsbeløbet kan ikke overstige 100.000 kr. pr. tilfælde.

Software: Informationssikkerhed og databeskyttelse

Krav til informationssikkerhed på 02.19 Fagsystemer (rammeaftale og dynamisk indkøbssystem) **er opdelt i pakker (grøn, gul, rød), som du vælger baseret på egen risikovurdering.**

Krav på 02.19 Fagsystemer omfatter følgende områder:

- Informationssikkerheds-politikker
- Organisering af informationssikkerhed
- Medarbejdersikkerhed
- Styring af aktiver
- Adgangsstyring
- Kryptografi
- Fysisk sikring og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Anskaffelse, udvikling og vedligeholdelse af systemer
- Leverandørforhold
- Styring af informationssikkerhedsbrud
- Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
- Overensstemmelse

På 02.19 Fagsystemer (dynamisk indkøbssystem) kan du:

- Tilpasse SKI's krav eller anvende egne sikkerhedskrav.
- Vedlægge databehandleraftale, når du offentliggør indkøbet.

På 02.19 Fagsystemer (rammeaftalen) har leverandøren accepteret databehandleraftale for de tilbudte services.

Krav- ID	Krav til leverandørforhold	ISO 27001-reference
15.1	Leverandøren skal sikre, at informationssikkerhedskrav til at minimere risici, der er forbundet med underleverandørers adgang til aktiver, relateret til Leveringskontraktens opfyldelse, aftales med Leverandøren og dokumenteres. Herunder skal Leverandøren sikre, at alle relevante informationssikkerhedskrav fastlægges og aftales med hver enkelt underleverandør, som kan få adgang til, behandle, lagre, kommunikere eller levere it-infrastrukturkomponenter til information i relation til Leveringskontraktens opfyldelse.	A.15.1.1 A.15.1.2
15.2	Leverandøren skal sikre, at aftaler med underleverandører indeholder krav til håndtering af informationssikkerhedsrisici, forbundet med tjenester og produkter for informations- og kommunikationsteknologi i relation til Leveringskontraktens opfyldelse. Herunder skal Leverandøren sikre at underleverandører orienterer Leverandøren om sikkerhedsbrud uden ugrundet ophold og i overensstemmelse med databehandleraftalen i øvrigt.	A.15.1.3
15.3	Leverandøren skal regelmæssigt overvåge, gennemgå og auditere underleverandørydelser, der anvendes til Leveringskontraktens opfyldelse, og påse disse underleverandørydelsers overensstemmelse med de indgåede underleverandøraftaler.	A.15.2.1
15.4	Leverandøren skal sikre, at ændringer af underleverandørydelser, herunder vedligeholdelse og forbedring af eksisterende informationssikkerhedspolitikker, -procedurer og -kontroller, styres, under hensyntagen til hvor kritiske de involverede forretningsinformationer, -systemer og -processer er, og til en revurdering af risici i relation til Leveringskontraktens opfyldelse.	A.15.2.2

SKI's teleaftaler: Informationssikkerhed og databeskyttelse

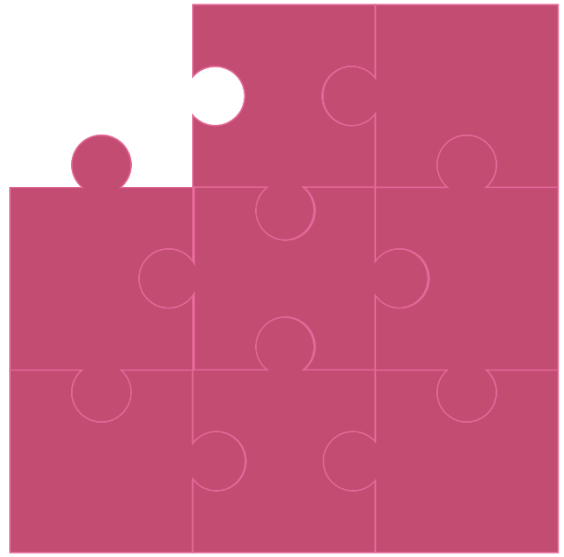
- Sikkerhedskrav i 50.48 Tele og data (rammeaftale) – **SKI's fastsættelse af sikkerhedskrav**
  - Samarbejde med Styrelsen for Samfundssikkerhed (SAMSIK) – vurdering af risici
  - Kritisk infrastruktur – sektorens modenhed
  - Kravene er obligatoriske
  - Fokus på netsikkerhed, trusselsbeskyttelse, logning og overvågning

Indholdsfortegnelse

Hvad skal du selv gøre?

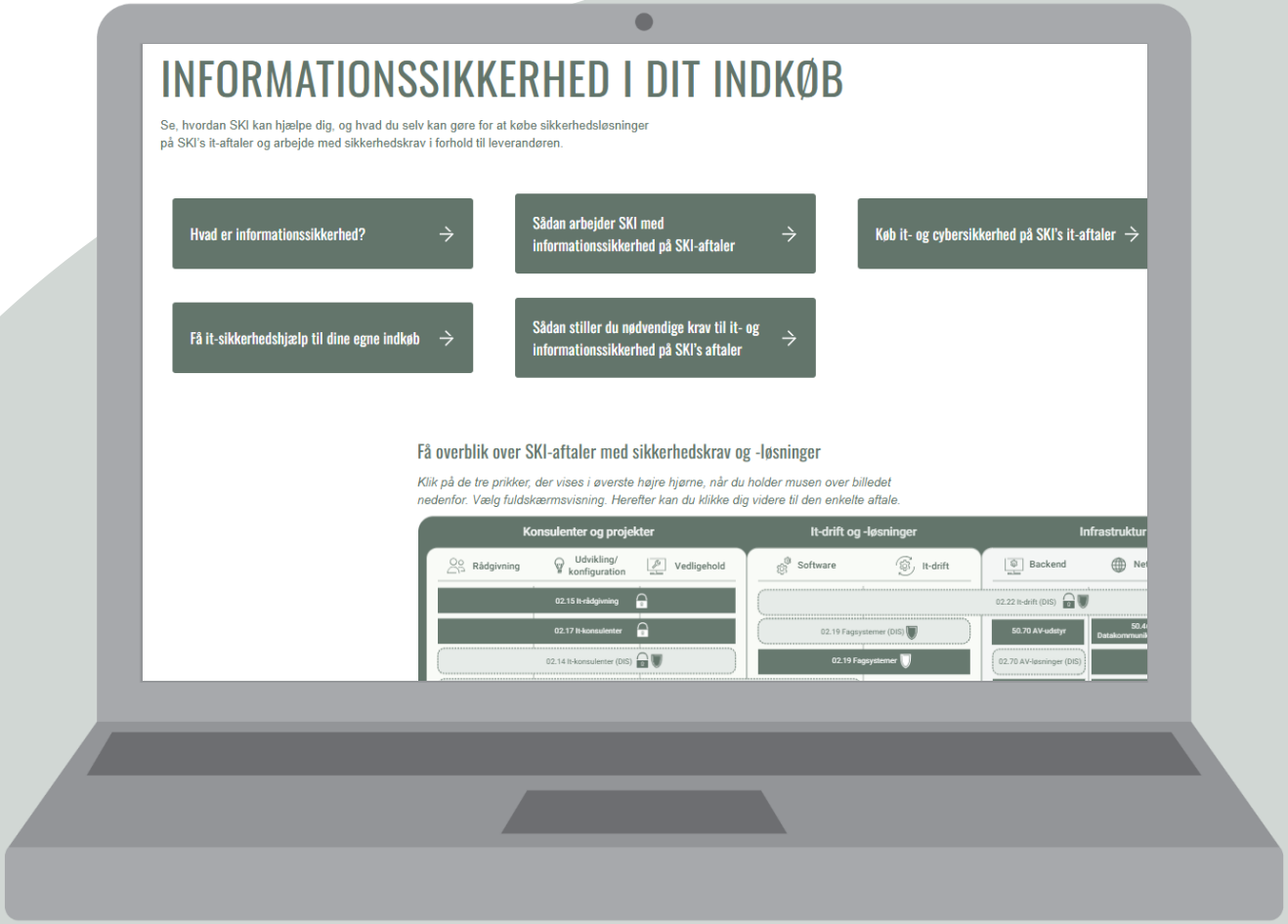
Med SKI får du et solidt sikkerhedsfundament i aftalerne, men den enkelte offentlige organisation skal selv:

- Foretage en risikovurdering af egne it-systemer og leverandører
- Vurdere, hvor kritiske systemerne er for driften
- Overveje konsekvenserne ved leverandørsvigt
- Beslutte, om der er behov for supplerende krav - fx om kryptering, adgangsstyring eller responstider
- Føre løbende tilsyn med, at leverandøren overholder kravene
- Styrelsen for Samfundssikkerhed: Her findes bl.a. vejledning, der skal hjælpe med at implementere NIS2



Viser risikovurderingen, at der er behov for supplerende sikkerhedskrav, kan disse stilles i SKI's dynamiske indkøbssystemer.

Få hjælp til dit arbejde med informationssikkerhed på ski.dk



Spørgsmål og afslutning

?

Besøg ski.dk

SKI