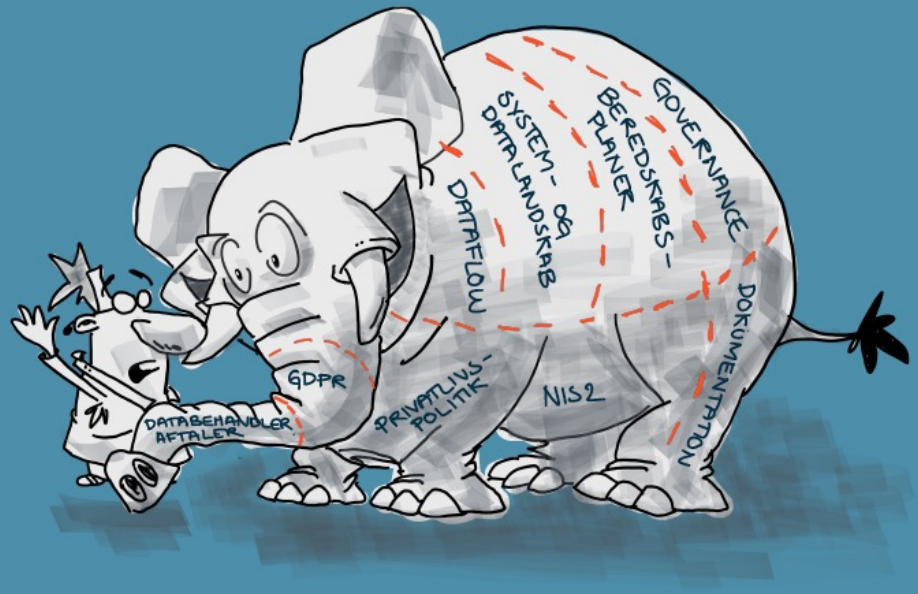
LAKESIDE

IT-COMPLIANCE

+ TECH CITY AARHUS

Hypotese

It-compliance opgaven kan virke stor og uoverskuelig som en elefant.



LAKESIDE

[kʌmˈplajəns]

En bitter pille eller god medicin?

Compliance

1) Overholdelse af regler; efterlevelse af retningslinjer
   Synonym: efterlevelse

2) En patients efterlevelse af de anbefalinger vedr. medicinindtagelse, diæt eller livsstilsændringer som et foreskrevet behandlingsforløb indebærer
   Synonymer: komplians, adhærens

(Kilde: Danske Ordbog – obs: /IKKE/ Ordbog over det danske Sprog ☺)

LAKESIDE

PROGRAM

14:30	Netværk og snacks
15:00	Velkommen og introduktion til emnet
15:10	Oplæg om risikovurderinger v. Geert Mikkelsen fra Alexandra Instituttet
15:35	Oplæg om beredskabsplaner v. Philippe Roy fra KMD
16:05	Oplæg om databehandleraftaler v. Mette Thøgersen fra Lakeside A/S
16:40	Opsamling på oplæg og dialog
17:00	Netværk og tapas

LAKESIDE

RISIKOANALYSE

Gert Læssøe Mikkelsen, Head of Security Lab.

Gert.l.Mikkelsen@Alexandra.dk

Sammen kommer vi #foran**digitalt**

ALEXANDRA INSTITUTTET

Uvildig forsknings-baseret rådgivning og udvikling

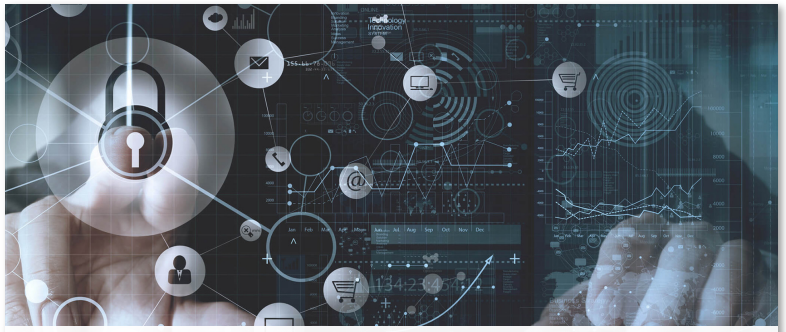
- Vores tid er fordelt ca. 50/50 mellem **anvendt forskning** og **kommercielle projekter**.
- Det er din garanti for, at vi har den forskningsfaglige dybde, der kræves for at skabe fremtidssikre digitale teknologier og services.

Sammen om fremtidens digitale Danmark

Kom foran digitalt

IOT OG SMARTE PRODUKTER

DIGITAL GRØN OMSTILLING



CYBERSIKKERHED

KUNSTIG INTELLIGENS

DIGITAL SUNDHED

COMPUTERGRAFIK, VISION OG SIMULERING

Baggrund

INDUSTRIENS FOND

ALEXANDRA INSTITUTTET

Dansk Industri

DANSK ERHVERV

Erhvervshus MIDTJYLLAND

DTU

AALBORG UNIVERSITET

Hvorfor risikostyring?

- “Perfekt” cybersikkerhed findes ikke

Hvorfor risikostyring?

- **Security vs. Safety**

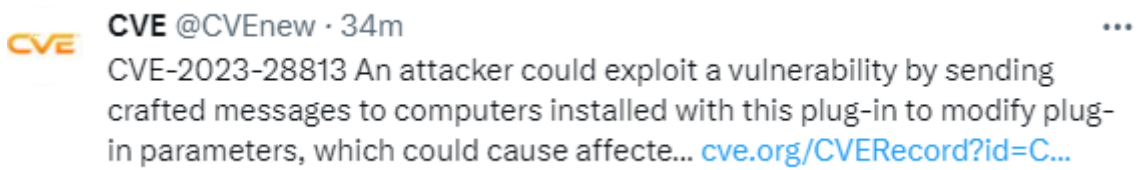
Afskærmninger, der er indrettet til at beskytte personer mod farer som følge af bevægelige, kraftoverførende dele skal være:

— enten faste afskærmninger, som omhandlet i punkt 1.4.2.1, eller

— bevægelige afskærmninger med tvangskobling, som omhandlet i punkt 1.4.2.2.

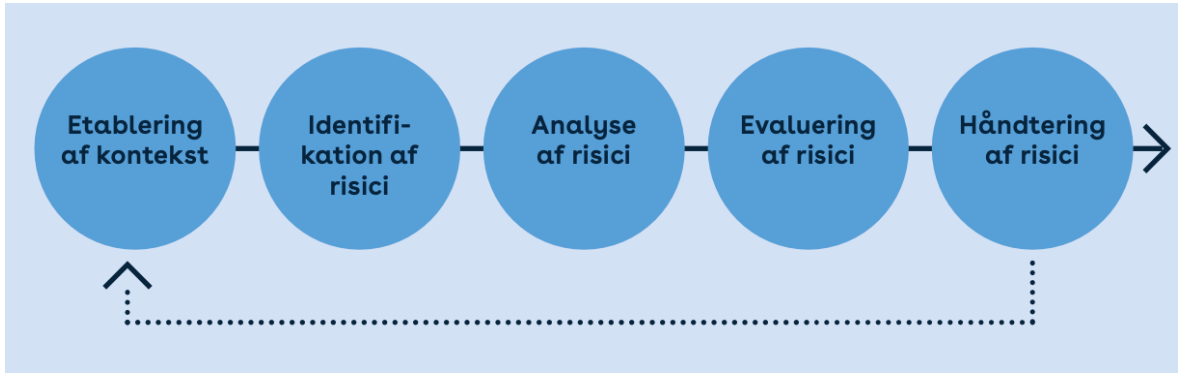
Bevægelige afskærmninger med tvangskobling bør benyttes, når det forventes, at der ofte skal foretages indgreb.

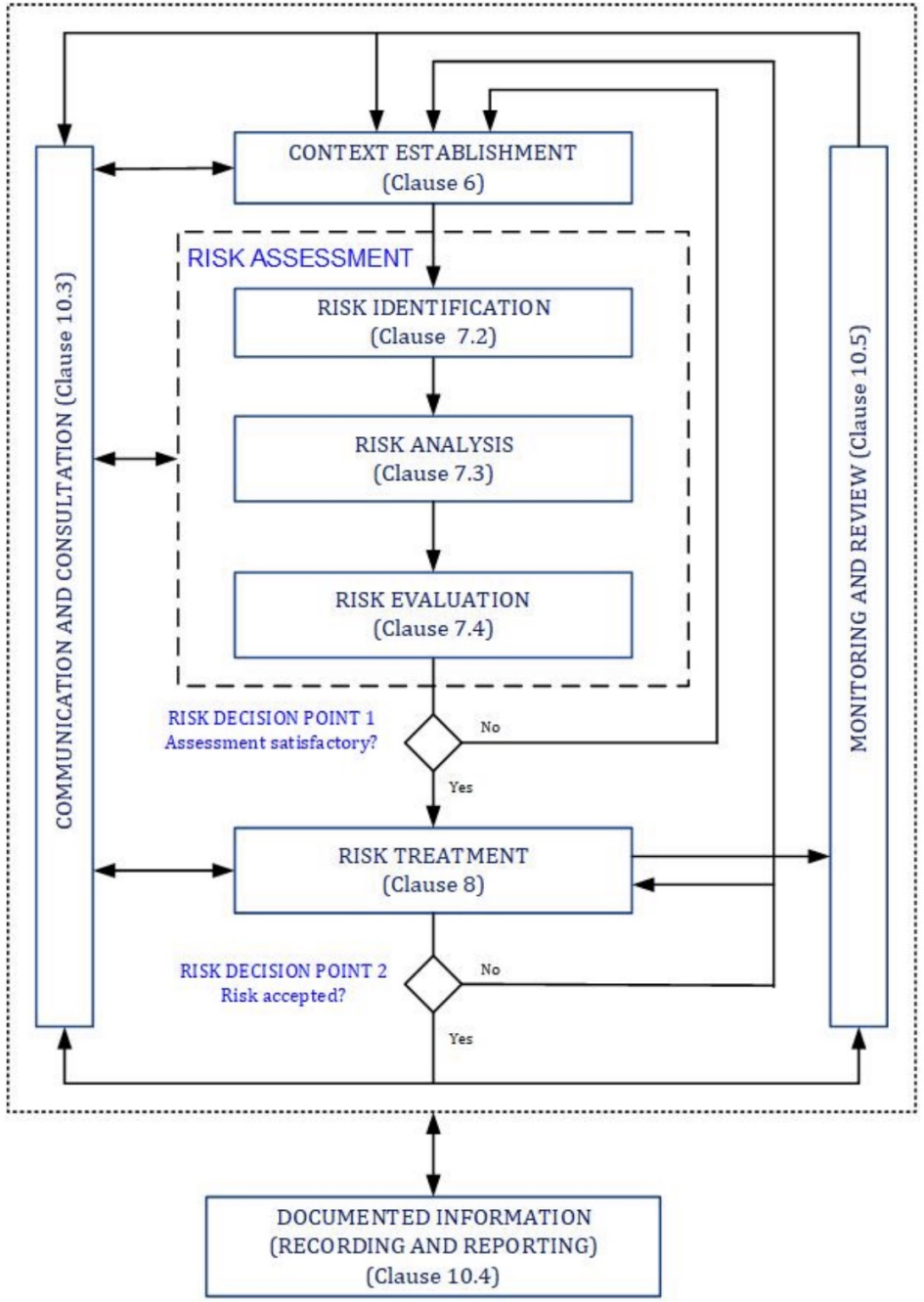
VS.



Alle laver risikoanalyser

Riskostyrings-processen





Før selve analysen - Kontekst

- Hvad handler sikkerhed om for virksomheden?
  - Er der særlige hensyn?
  - Hvad kan vi tåle?

Konteksten – valg af metode

Konsekvens – brug en logaritmisk skala:

- Meget lav: 1-10
- Lav: 10-100
- Høj: 100-1000
- Meget høj: 1000+

Sandsynlighed eller frekvens?

- Meget lav: 0,01 % eller 100 års hændelse
- Lav: 0,1 % eller 10 års hændelse
- Høj: 1 % eller års hændelse
- Meget høj: 1+% eller flere gange årligt

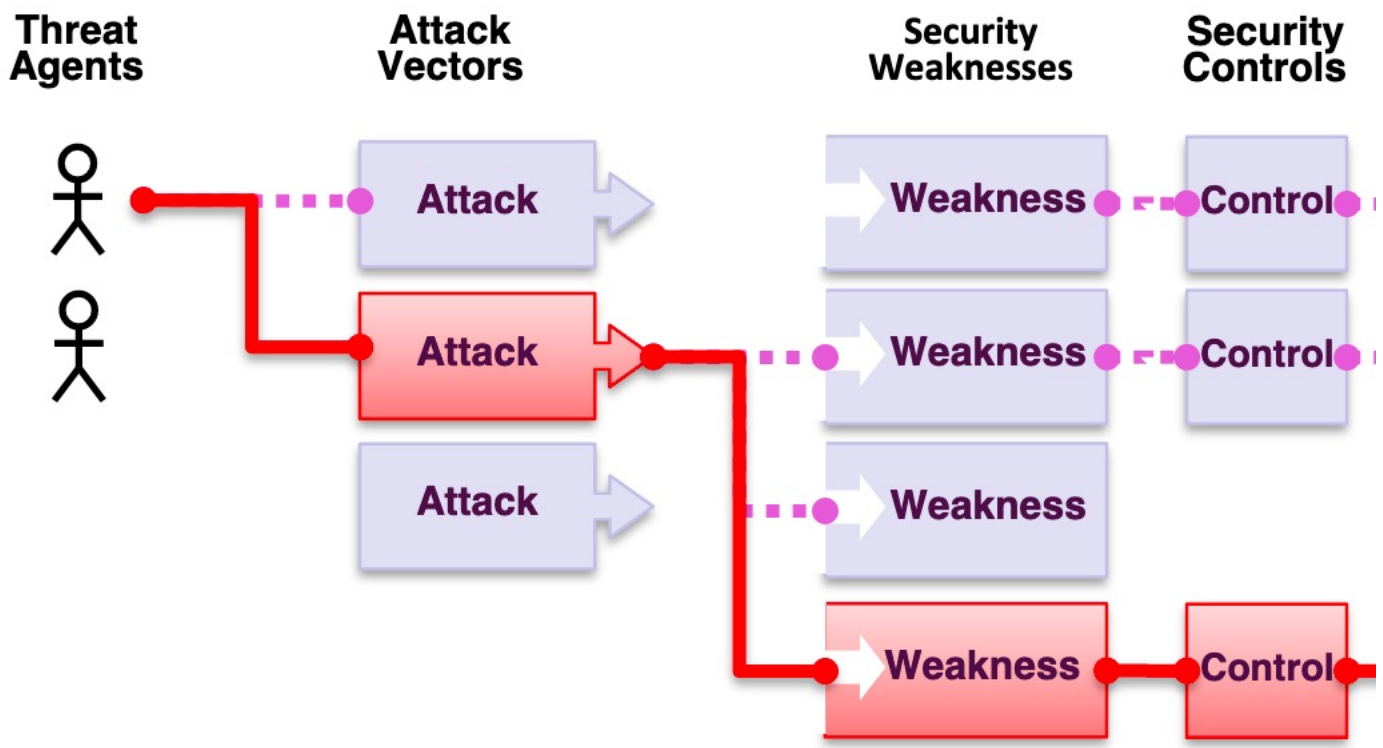
Risiko: Hvad og hvordan

Risiko = Sandsynlighed x Konsekvens

Tabel B3

KONSEKVENS	SANDSYNLIGHED				
	10-års hændelse	Årligt	Kvartalsvist	Ugentligt	Dagligt
0-50.000 kr.	1	2	3	4	5
50.001-125.000 kr.	2	4	6	8	10
125.001-500.000 kr.	3	6	9	12	15
500.001-2.500.000 kr.	4	8	12	16	20
2.500.001+ kr.	5	10	15	20	25

Risiko – sandsynlighed



Agenten:

- Motivation
- Kompetencer
  - Teenager
  - Organisede kriminelle
  - Fjendtlige nationer
  - Konkurrenter
  - Et mix

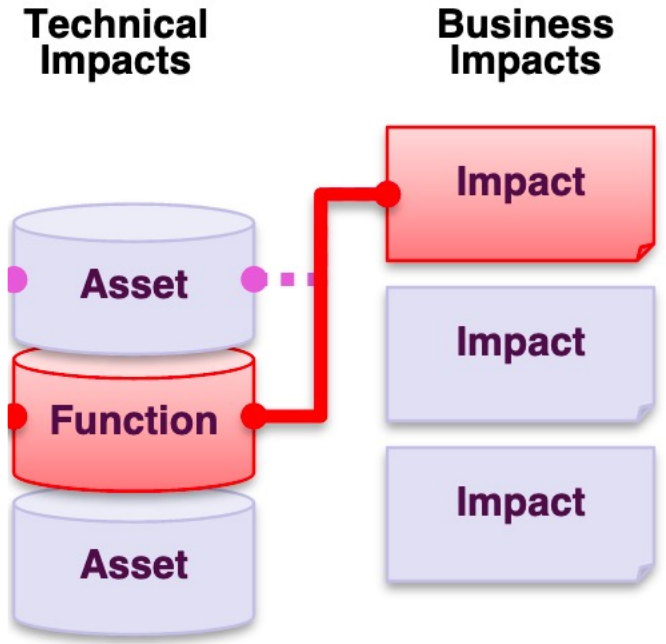
Styrke af systemet :

- Undgå svagheder
- Sikkerhedskontroller

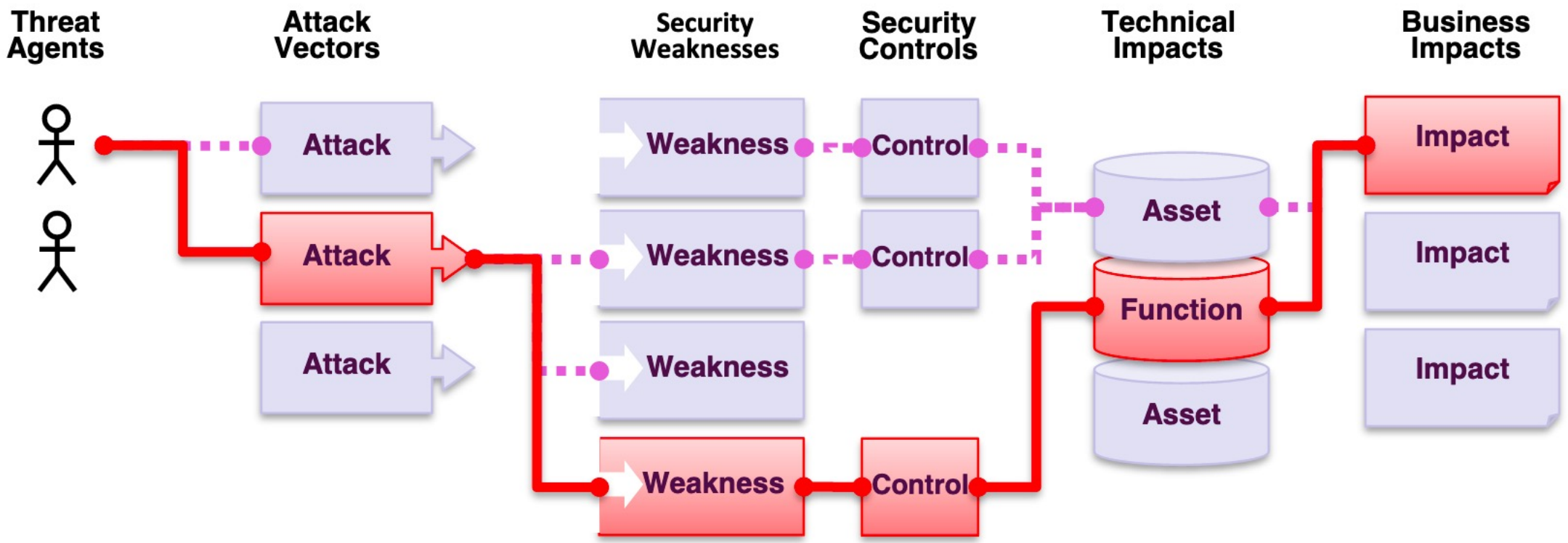
Risiko – Konsekvensen

- Teknisk konsekvens
  - Uautoriseret adgang til data
  - Uautoriseret adgang til funktion
  - Ødelægge noget
  - …
- Forretning
  - Tab af kunder
  - Bøder
  - Tid og ressourcer for at rydde op
  - …

- C – Confidentiality
- I – Integrity
- A – Availability

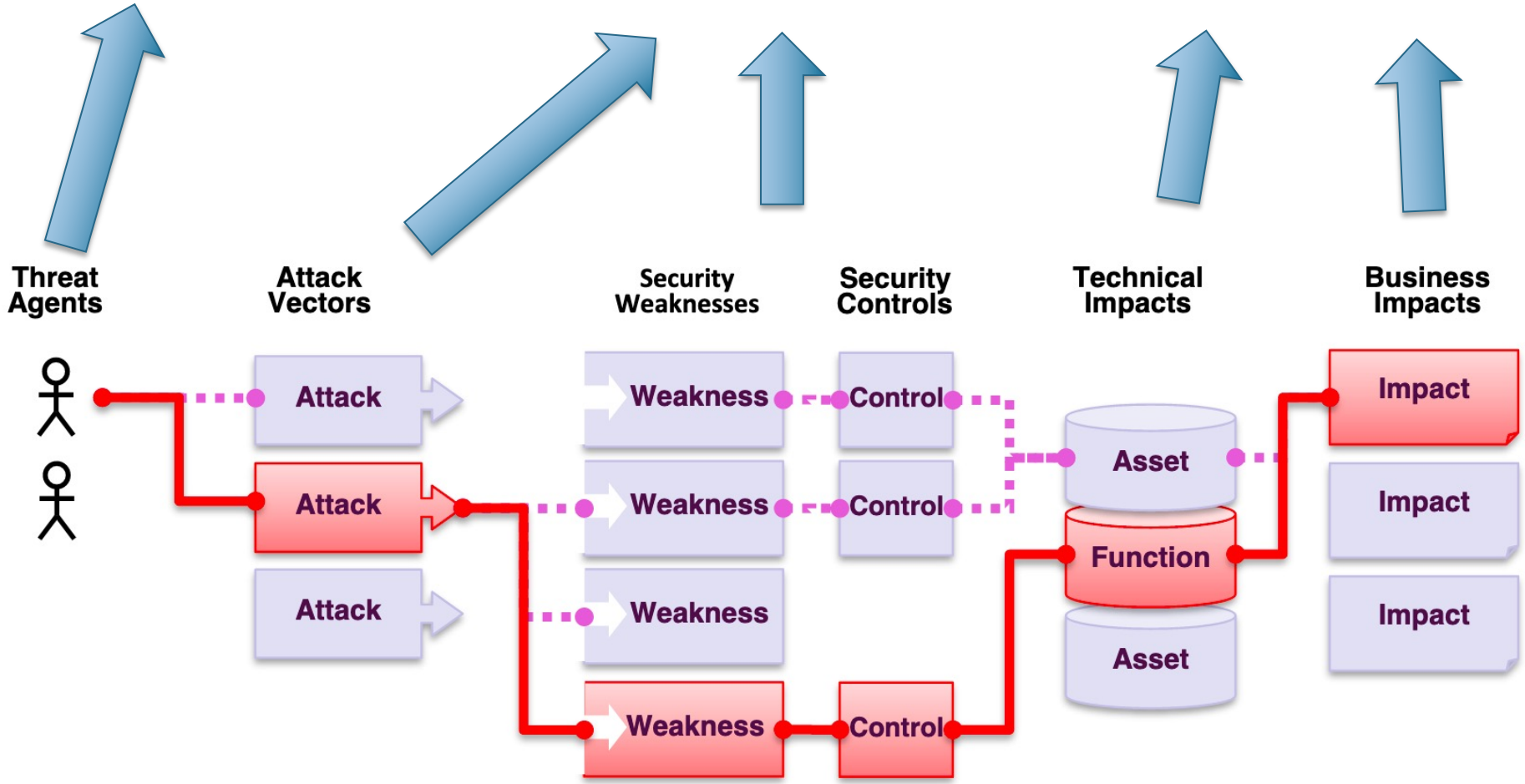


Risiko


Threat Agents
Attack Vectors
Security Weaknesses
Security Controls
Technical Impacts
Business Impacts
Attack
Attack
Attack
Weakness
Weakness
Weakness
Weakness
Control
Control
Control
Asset
Function
Asset
Impact
Impact
Impact

Skabelon for en risiko:

- "***Trusselsaktør*** udfører ***trussel*** for at ***konsekvens af truslen***"



Et par eksempler

- "***Bulgarske hackere*** anvender ***phishing mails*** for at kompromittere medarbejderes laptops og ***installerer ransomware på lokale og delte drev***"

- "***Aktivister*** lancerer ***DDoS kampagne*** mod firmaets offentlige hjemmeside og ***gør webshoppen utilgængelig***"

Et par eksempler

- “***Bulgarske hackere*** anvender ***phishing mails*** for at kompromittere medarbejderes laptops og ***installerer ransomware på lokale og delte drev***”

- Sandsynlighed = Lav (2)
- Konsekvens = Høj (3)
- Risiko = 2 x 3 = 6

Aktiver

- Beskriv Aktiver

Konsekvens

- Konsekvens (C,I,A)

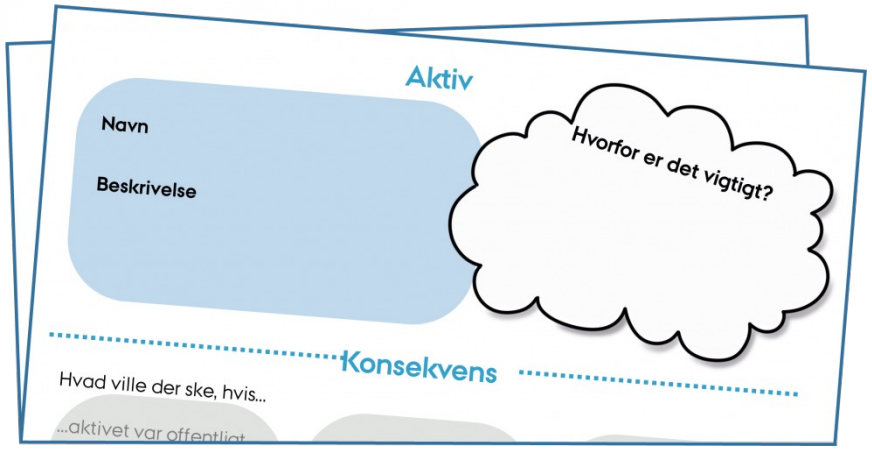
Trusler

- Risiko for aktiv

- C – Confidentiality
- I – Integrity
- A – Availability

Tabel B3

KONSEKVENS	SANDSYNLIGHED				
	10-års hændelse	Årligt	Kvartalsvist	Ugentligt	Dagligt
0-50.000 kr.	1	2	3	4	5
50.001-125.000 kr.	2	4	6	8	10
125.001-500.000 kr.	3	6	9	12	15
500.001-2.500.000 kr.	4	8	12	16	20
2.500.001+ kr.	5	10	15	20	25



https://da.dbd.au.dk/p/toolbox#iot-cyber-sikkerhed

Kom videre:

Generel modstandsdygtighed
inkl. cybersikkerhed:

MODSTANDSDYGTIG

modstandsdygtig.dk

(eller kontakt Gert)

IoT Cybersikkerhed
Kurser – udviklingsprojekter

cybersikker.alexandra.dk

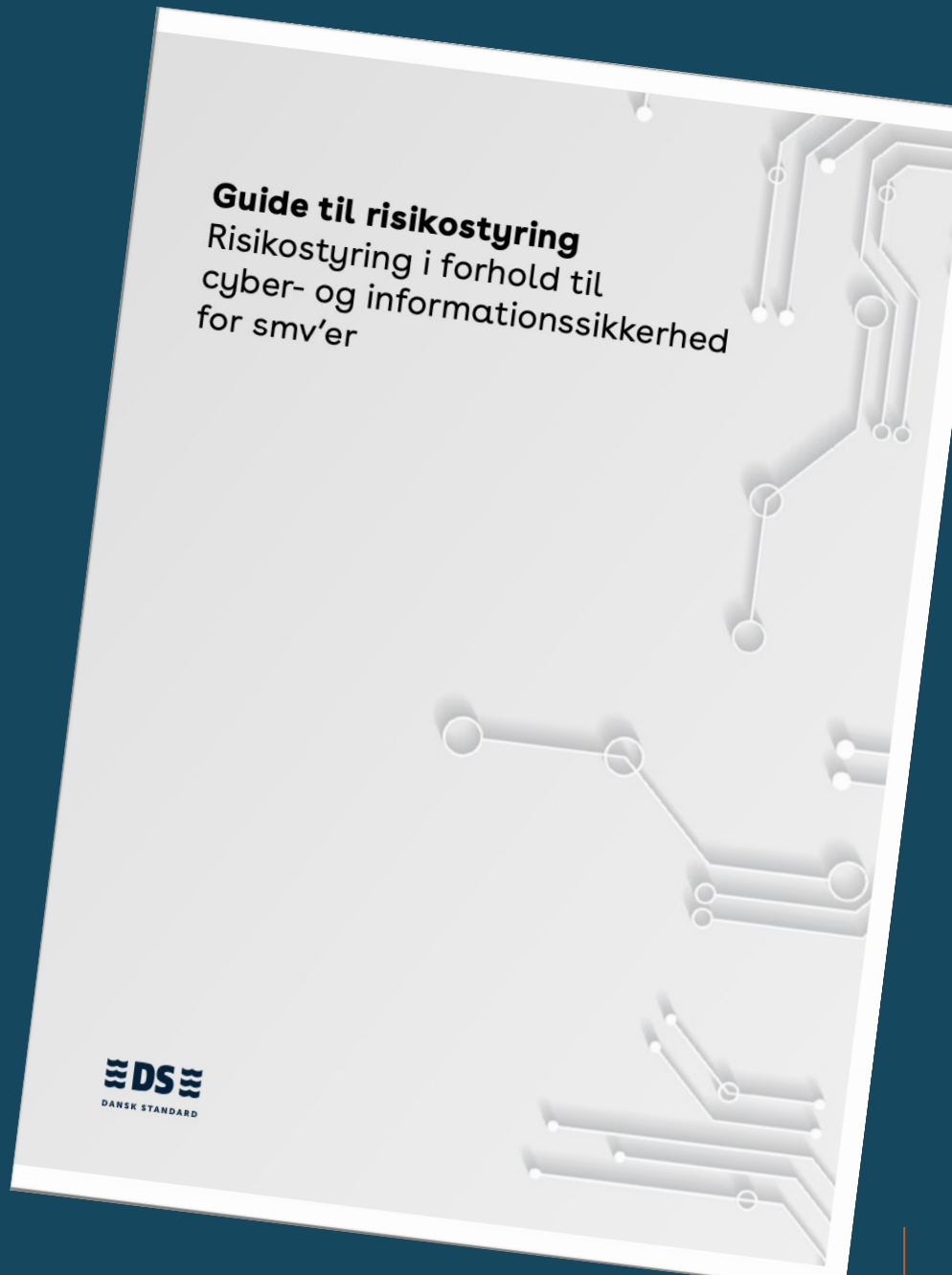
INDUSTRIENS FOND

Kom selv videre

- Guide til Risikostyring:
  Dansk Standard – ds.dk

- IoT cybersikkerhed:
  https://cybersikker.alexandra.dk
  https://da.dbd.au.dk/p/toolbox#iot-cyber-sikkerhed

- Security by Design:
  securitybydesign.alexandra.dk



KMD
An NEC Company

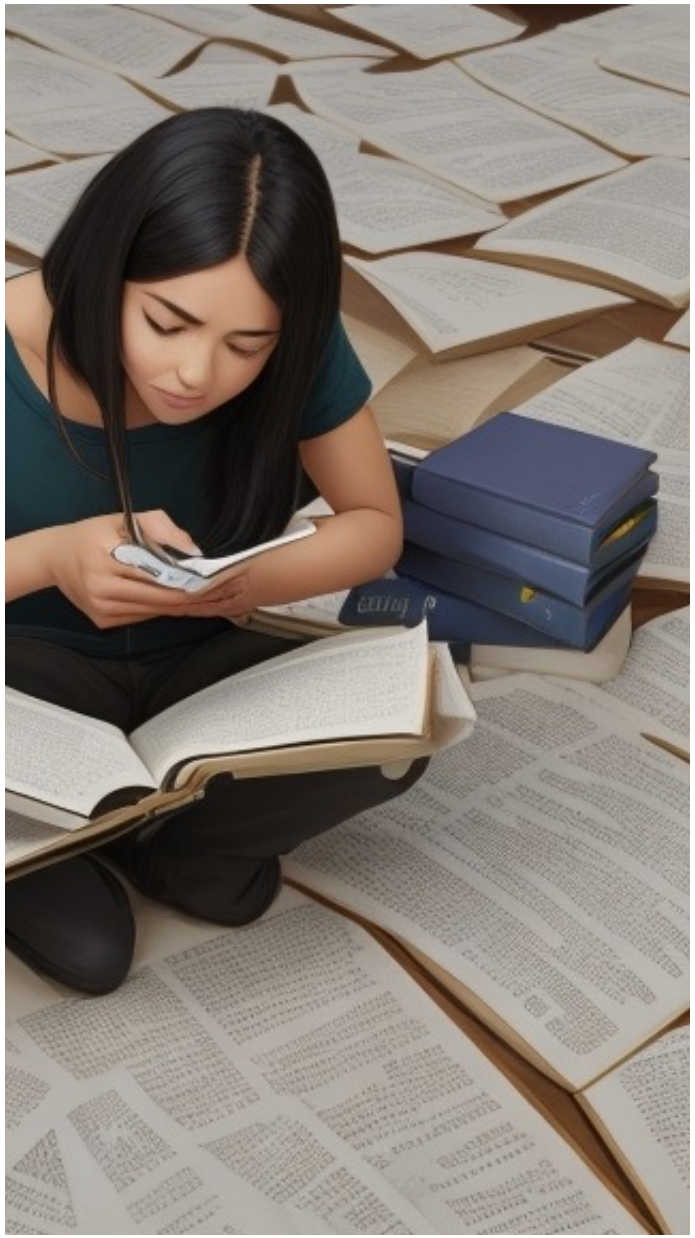
BEREDSKABSPLANER

WHAT IS IT GOOD FOR?

APRIL 2024

AGENDA – BEREDSKABSPLANER, WHAT IS IT GOOD FOR?

- **Definition – Hvad er en beredskabsplan?**
- **Less is (often) more**
- **Hvordan kommer man i gang?**
- **Must haves!**
- **Forbedringer**
- **Situationer fra virkeligheden**
- **Hvor kan man få hjælp?**
- **Værktøjer og råd**



DEFINITION – HVAD ER EN BEREDSKABSPLAN

- Hvad er beredskabsplaner?

beredskabsplan substantiv, fælleskøn

BØJNING -en, -er, -erne

UDTALE [be'ʁɛðˀsgabs-]

Betydninger

plan for foranstaltninger til afhjælpning af katastrofer, kriser, forurening el.lign.

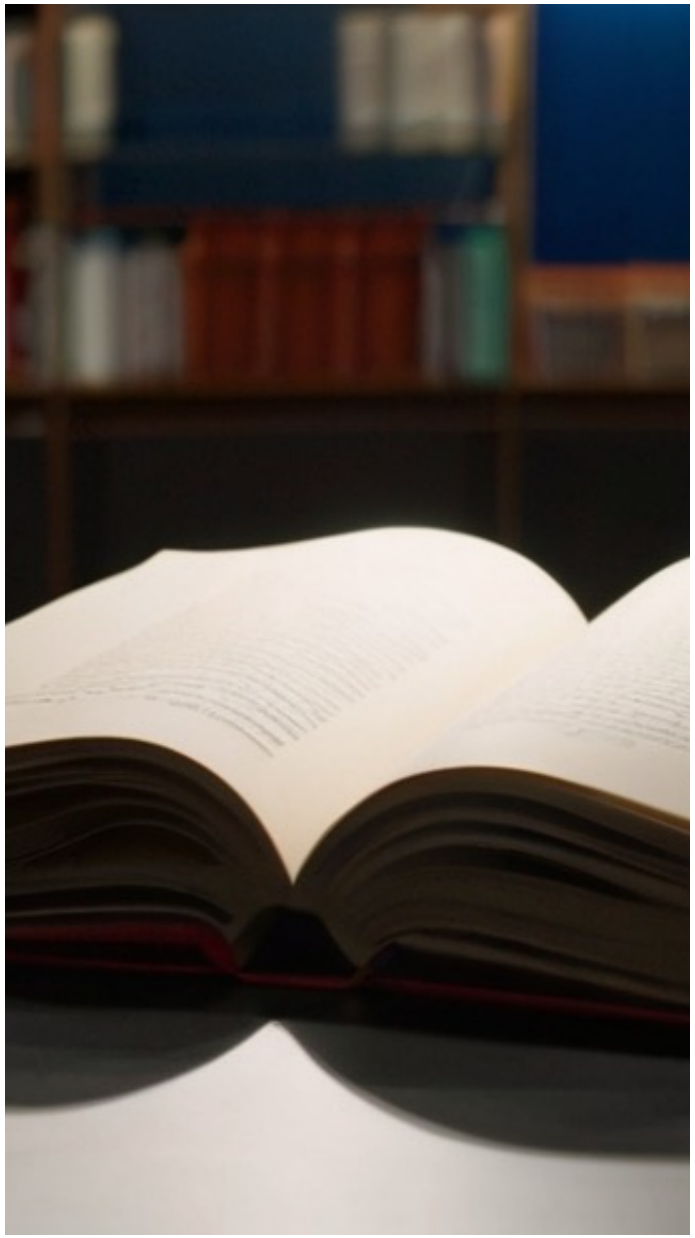
ORD I NÆRHEDEN beredskabsforanstaltning | nødberedskab | katastrofeberedskab | akutberedskab | redningsvæsen | bedriftværn...vis mere

OOA lagde vægt på at Miljøministeriet i sine beredskabsplaner for Barsebäck arbejdede med en sikkerhedszone på 80 km læreb1988

Rapportér et problem *fra Den Danske Ordbog*

https://ordnet.dk/ddo/ordbog?query=beredskabsplan

Billede genereret af Leonardo.ai



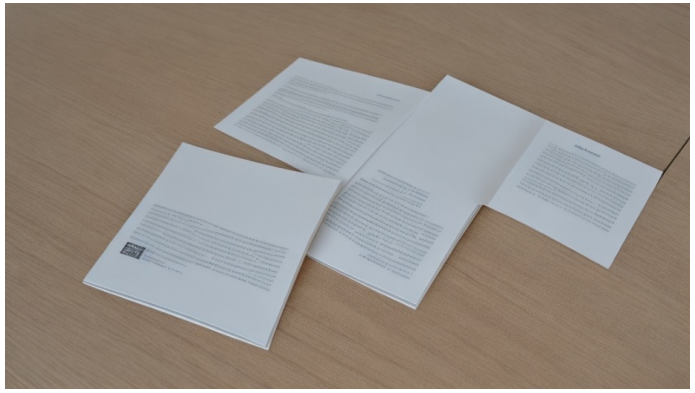
LESS IS (OFTEN) MORE

- En beredskabsplan er en vigtig dokument, der hjælper med at sikre sikkerhed og effektiv håndtering af nødsituationer.
- En beredskabsplan inden for IT, behøver ikke at tage højde for andet end IT.

  - Evakueringsplaner
  - Førstehjælp
  - Livrednings træning

Billede genereret af Leonardo.ai

HVORDAN KOMMER MAN I GANG?



Afgræns beredskabsplanen

- En beredskabsplan inden for IT, skal tage højde for IT.

Risikoanalyse

- Baser den på en risikoanalyse, er i afhængig af jeres hjemmeside virker, så bør DDoS nok være et scenarie i kigger på.

Kommunikationsplan

- Hvem siger hvad? Når pressen står udenfor og siger, har I nogle kommentarer? Hvem siger så hvad?

Genopretningsplaner for kritiske systemer

- Vær klar til at lade nogle systemer blive ved med at være nede, få jeres mest kritiske systemer op at køre igen. Resten må vente.

Ansvarsfordeling

- Find ud af hvem der gør hvad, for ellers løber alle rundt og antager at nogle gør noget.

MUST HAVES!

Dato

- Hvornår er dette dokument fra?

Version

- Er dette den nyeste version af planen?

System

- Hvilket system gælder denne plan for? Er det for kundedatabasen, eller hjemmesiden?

Link

- Er det muligt at finde den nyeste version på jeres intranet?

Ansvarlig for dokumentet

- Hvis dokumentet virker helt uoverskueligt, eller der er noget som ikke er helt klart, så kan det måske være godt at tale med en ven.

FORBEDRINGER?

Kriseberedskabs team

- De kalder ind, de tager notater, de fordeler opgaverne og holder folk op til opgaverne.

Børnepasning

- Hvordan gør man, hvis man har medarbejder der har børn der skal hentes? Nogle har faktisk tænkt det ind, så er der en anden medarbejder der henter børnene og tager dem med til arbejdet.

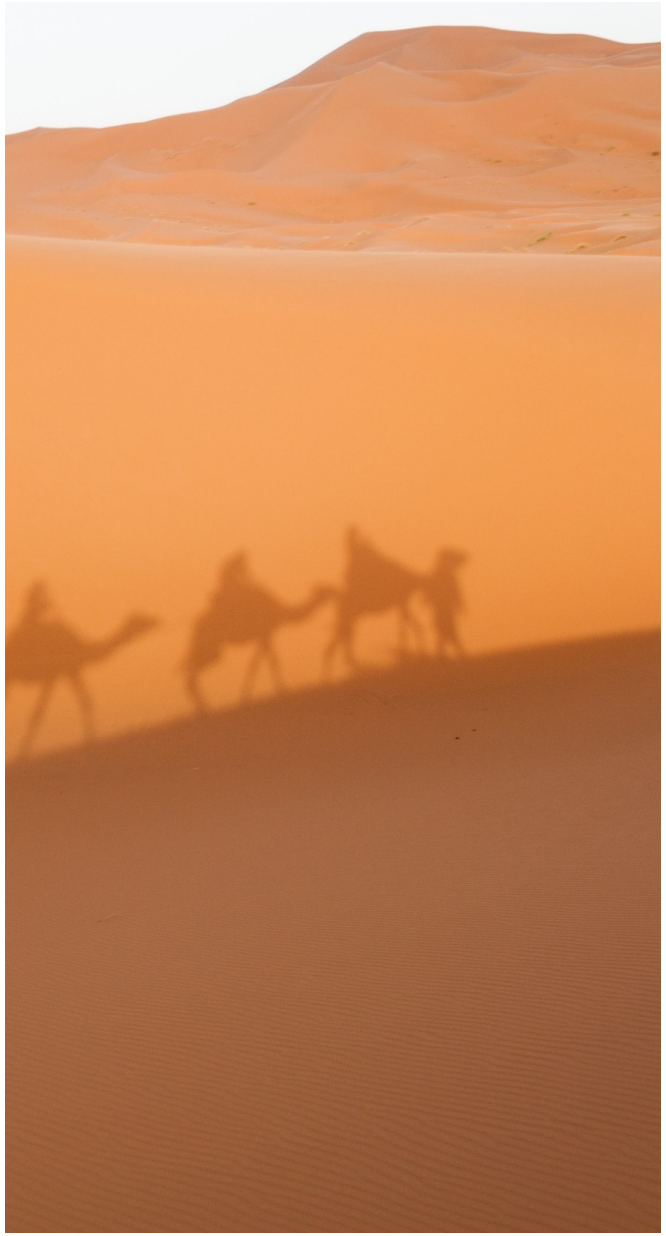
Mad

- Vi har alle brug for mad og kan ikke klare os uden

Feedback

- Efter krisen, bør i lære af krisen. Hvad virkede ikke? Men frem for alt, hvad virkede godt? Det kan måske komme nogle af jeres andre BCP´er tilgode.

Stock image



Stock image

SITUATIONER FRA VIRKELIGHEDEN

_ Hvad bør I kigger på lige nu?

- Lige nu er der to trusler vi ser nævnt i medierne.
  - 1) DDoS/DoS
  - 2) Ransomware
  - Har I ikke en BCP for disse bør I overveje det.

_ Hvor længe skal man beholde scenarierne i BCP´en?

- Kan nogle af jer huske fugleinfluenzaen fra 2008?
  - Den hoppede først til kameler i Mellemøsten, og derfra til mennesker
  - Der var frygt for en global pandemi
  - BCP´en blev opdateret med, vaccine planer for nøgle medarbejder, hjemmearbejdspladser- monitor og laptops, mulighed for indkøb af madvarer der blev stillet ved medarbejdernes hoveddør, isolering
  - Det dannede grundlag for en krise håndtering af COVID-19 i 2020.

HVOR KAN MAN FÅ HJÆLP?

Det er muligt at få hjælp

- Nogle gang skal man betale for det.

Andre gange kan man få hjælp

- Vi får meget for vores skattepenge i Danmark.

- https://www.cfcs.dk/da/temasider/tiltag-til-styrket-cyberberedskab/

- https://sikkerdigital.dk/myndighed/iso-27001-implementering/beredskabsstyring/implementering

CFCS / Temasider

Tiltag til styrket cyberberedskab

Center for Cybersikkerhed har samlet en oversigt over en række tiltag, som organisationer kan bruge til at identificere indsatsområder for den grundlæggende cybersikkerhed.

Det er vigtigt at have en række grundlæggende foranstaltninger og processer på plads for at imødegå cyberangreb. Selvom sådanne tiltag er basale, så udgør de fundamentet for et solidt cyberforsvar.

Center for Cybersikkerhed (CFCS) har samlet en oversigt over en række tiltag, som organisationer kan bruge i deres arbejde med at sikre, at fundamentet er på plads til at bygge yderligere foranstaltninger ovenpå. Tiltagene bygger på eksisterende vejledninger og best practice, men oversigten er ikke udtømmende.

CFCS anbefaler alle organisationer at have nedenstående tiltag for øje:

1. Beredskabsplanlægning og krisestyring

Gennemgå og afprøv organisationens beredskabsplaner, herunder nødplaner mhp. at sikre, at:
1.1. Beredskabsplaner er opdaterede.
1.2. Kontaktoplysninger og -lister er opdaterede.
1.3. Alle relevante personer er bekendt med beredskabsplanen og deres ansvar og rolle i beredskabet.
1.4. Beredskabsplaner mv. er tilgængelige offline.
1.5. Kommunikationsmidler fungerer, hvis it-systemer er utilgængelige.

HVOR KAN MAN FÅ HJÆLP?

Det er muligt at få hjælp

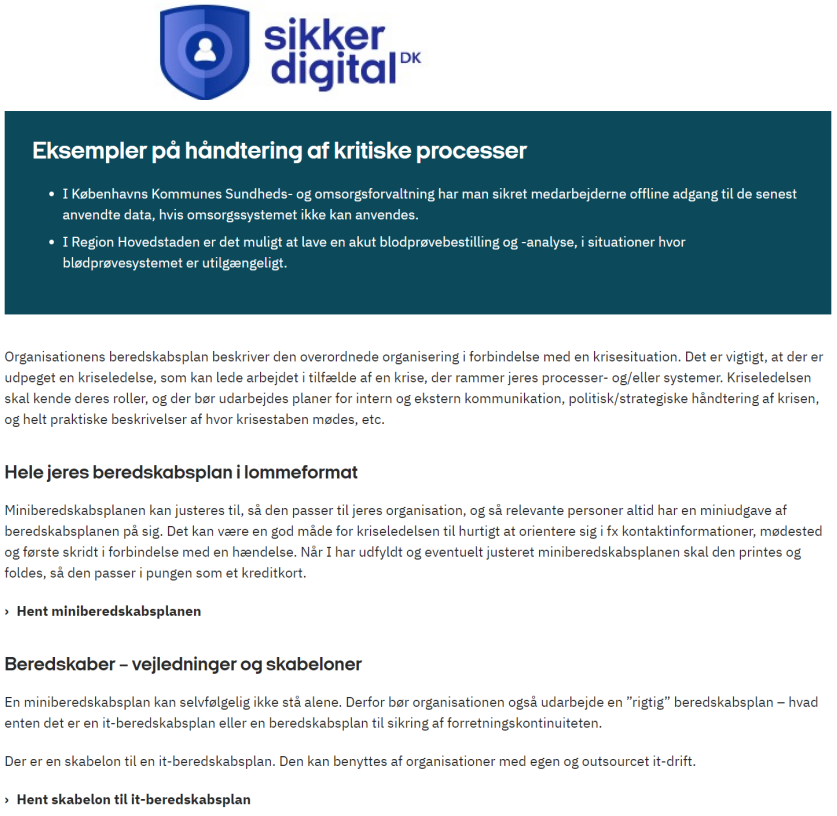
- Nogle gang skal man betale for det.

Andre gange kan man få hjælp

- Vi får meget for vores skattepenge i Danmark.

- https://www.cfcs.dk/da/temasider/tiltag-til-styrket-cyberberedskab/

- https://sikkerdigital.dk/myndighed/iso-27001-implementering/beredskabsstyring/implementering



sikker digital DK

Eksempler på håndtering af kritiske processer

- I Københavns Kommunes Sundheds- og omsorgsforvaltning har man sikret medarbejderne offline adgang til de senest anvendte data, hvis omsorgssystemet ikke kan anvendes.
- I Region Hovedstaden er det muligt at lave en akut blodprøvebestilling og -analyse, i situationer hvor blødprøvesystemet er utilgængeligt.

Organisationens beredskabsplan beskriver den overordnede organisering i forbindelse med en krisesituation. Det er vigtigt, at der er udpeget en kriseledelse, som kan lede arbejdet i tilfælde af en krise, der rammer jeres processer- og/eller systemer. Kriseledelsen skal kende deres roller, og der bør udarbejdes planer for intern og ekstern kommunikation, politisk/strategiske håndtering af krisen, og helt praktiske beskrivelser af hvor krisestaben mødes, etc.

Hele jeres beredskabsplan i lommeformat

Miniberedskabsplanen kan justeres til, så den passer til jeres organisation, og så relevante personer altid har en miniudgave af beredskabsplanen på sig. Det kan være en god måde for kriseledelsen til hurtigt at orientere sig i fx kontaktinformationer, mødested og første skridt i forbindelse med en hændelse. Når I har udfyldt og eventuelt justeret miniberedskabsplanen skal den printes og foldes, så den passer i pungen som et kreditkort.

› **Hent miniberedskabsplanen**

Beredskaber – vejledninger og skabeloner

En miniberedskabsplan kan selvfølgelig ikke stå alene. Derfor bør organisationen også udarbejde en "rigtig" beredskabsplan – hvad enten det er en it-beredskabsplan eller en beredskabsplan til sikring af forretningskontinuiteten.

Der er en skabelon til en it-beredskabsplan. Den kan benyttes af organisationer med egen og outsourcet it-drift.

› **Hent skabelon til it-beredskabsplan**

Kan man gøre noget for at forhindre at man bliver ramt af et nedbrud?

Ja det er muligt at gøre noget.

Hvis budgettet ikke tillader store investeringer, hvad kan man så gøre?

Patch management

https://heimdalsecurity.com/

Ad(og meget andet)blocker

https://pi-hole.net/

God guide

https://www.crosstalksolutions.com/the-worlds-greatest-pi-hole-and-unbound-tutorial-2023/

Block lists

https://firebog.net/

Desuden mener jeg at Karthago bør jævnes med Jorden

DMARC

Få oprette en DMARC Record, og sæt den til reject

Details

v=DMARC1; p=none; rua=mailto:izjjda8f@ag.eu.dmarcian.com; ruf=mailto:izjjda8f@fr.eu.dmarcian.com;

To understand and fix the specific errors, use our DMARC Inspector.

Kig også på jeres SPF record

Her er det muligt at sende mails fra op til 248.908 IP´er.

```
v=spf1 include:spf.mailanyone.net include:sendgrid.net include:spf.hatteland.com include:_spf.etrack1.com include:servers.mcsv.net a:zgateway.zuora.com a:mail1.dialogportal.com ip4:64.79.155.0/24 ip4:207.218.90.0/24 -all
```

Wikipedia

Desuden mener jeg at Karthago bør jævnes med Jorden

Details

v=DMARC1; p=none; rua=mailto:izjjda8f@ag.eu.dmarcian.com; ruf=mailto:izjjda8f@fr.eu.dmarcian.com;

To understand and fix the specific errors, use our DMARC Inspector.

Kig også på jeres SPF record

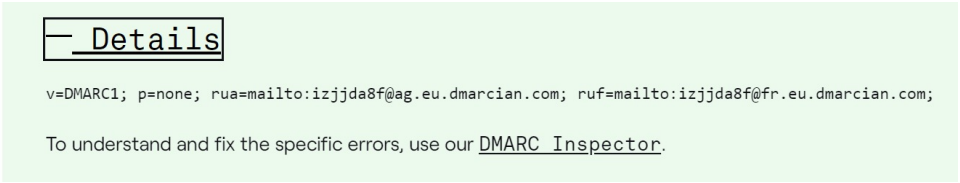
Her er det muligt at sende mails fra op til 248.908 IP´er.

```
v=spf1 include:spf.mailanyone.net include:sendgrid.net include:spf.hatteland.com include:_spf.etrack1.com include:servers.mcsv.net a:zgateway.zuora.com a:mail1.dialogportal.com ip4:64.79.155.0/24 ip4:207.218.90.0/24 -all
```

Desuden mener jeg at Karthago bør jævnes med Jorden

DMARC

Få oprette en DMARC Record, og sæt den til reject




```
v=spf1 include:spf.mailanyone.net include:sendgrid.net include:spf.hatteland.com include:_spf.etrack1.com include:servers.mcsv.net a:zgateway.zuora.com a:mail1.dialogportal.com ip4:64.79.155.0/24 ip4:207.218.90.0/24 -all
```

SPØRGSMÅL ?

Hvis i har spørgsmål, kan I enten sende dem nu,
eller tage fat i mig bagefter.

- Philippe Roy
- phr@kmd.dk
- +45 23 84 76 85

DATABEHANDLING? HVAD SÅ?

LAKESIDE

INDHOLD

LAKESIDE

DATATILSYNETS KLASSIFIKATION AF PERSONOPLYSNINGER

Desuden defineres **'fortrolige oplysninger'**

CPR-nr er en fortrolig oplysning.

Det afgørende for, om en oplysning skal anses for fortrolig, vil være en vurdering af, om oplysningen efter den almindelige opfattelse i samfundet bør være utilgængelig for offentlighedens kendskab, jf. straffelovens § 152 sammenholdt med forvaltningslovens § 27. Følsomme personoplysninger vil utvivlsomt være fortrolige oplysninger. Omvendt er en fortrolig oplysning kke altid følsom.

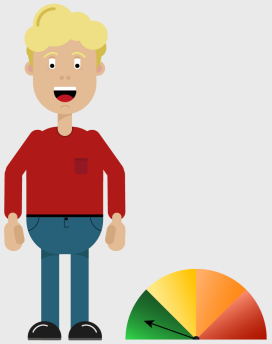
Ikke-følsomme personoplysninger kan i visse situationer være fortrolige. Det gælder efter omstændighederne oplysninger om indtægts- og formueforhold, arbejds-, uddannelses- og ansættelsesmæssige forhold. Det samme gælder oplysninger om interne familieforhold, herunder oplysninger om f.eks. selvmordsforsøg og ulykkestilfælde. Oplysninger, der kan henføres til bestemte personer, og som ikke kan nægtes udleveret efter offentlighedsloven, vil ikke være af fortrolig karakter. Det gælder f.eks. oplysninger af rent objektiv karakter, såsom oplysninger om udstedelse af pas, kørekort, jagttegn mv

LAKESIDE

DATAMANDEN
EN KLASSIFIKATION AF DATA

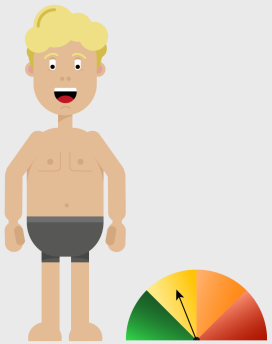
Datamanden er en infografik af datatyper og deres klassifikation. Afklædningen af Datamanden illustrerer at graden af følsomhed stiger ved indsamling og anvendelsen af de forskellige data.

Barometret indikerer hvorvidt konsekvenser og krav til beskyttelse er lav (grøn), middel (gul), høj (orange) eller meget høj (rød)



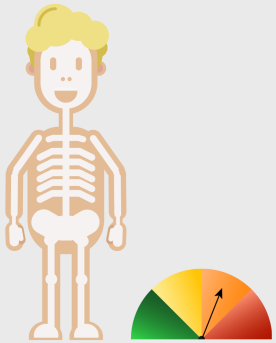
INFORMATION

Skostørrelse, øjenfarve, køn, højde, hårfarve, interesser, alder, profession, ”likes”



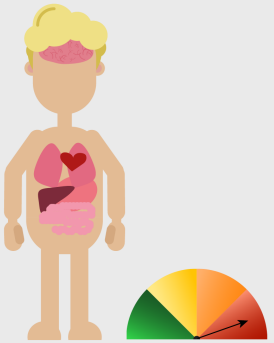
PERSONDATA

Email, telefonnummer, nummerplade, adresse, Pseudonymiseret data, navn, IP adresse



FORTROLIG DATA

CPR nummer



FØLSOM DATA

Religion, seksualitet, fagforening, blodtype, etnicitet, handicap, graviditet, fingeraftryk, billede, DNA

LAKESIDE

Delingsniveau	Persondatakategori	Typer af registreret	Lakesides interne data
4 - Hemmelige	**Følsomme personoplysninger**	Ansatte	* Personalesager * Helbredsoplysninger
		Ansøgere	* Ansøgninger
	Information om strafforhold	Ansatte	* Straffeattester
3 - Skærpet internt fortrolige	**Fortrolige personoplysninger**	Ansatte	* CPR-nr
	Almindelige personoplysninger	Ansatte	* Ansættelseskontrakter * Lønoplysninger * Bankoplysninger
2 - Internt fortrolige	**Almindelige personoplysninger**	Ansatte	* Familierelationer / historier om medarbejdere * Billeder (taget i firmaregi men ikke til offentliggørelse) * Adresseoplysninger mv. på medarbejdere
		Kunders ansatte	* Navn * Firma e-mail * Stillingsbetegnelse * Telefonnummer (kan være privatnummer)
		X-ray deltagere	* Navn * Firma e-mail
1 - Delte	**Almindelige personoplysninger**	Ansatte	* CV'er
0 - Offentlig oplysninger	**Almindelige personoplysninger**	Ansatte	* Navn * Firma e-mail * Stillingsbetegnelse * Telefonnummer (kan være privatnummer) * Billede

DATABEHANDLING

En behandling kan efter databeskyttelsesforordningen omfatte enhver håndtering af personoplysninger, herunder indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse. (Datatilsynet)

ROLLER

Dataansvarlig

Bestemmer, med hvilke formål personoplysningerne må behandles (formålet), og hvordan person-oplysningerne må behandles (hjælpemidlerne), herunder af hvem personoplysningerne må behandles

Databehandler

Udfører databehandling på vegne af en Dataansvarlig – under instruks

Serviceleverandør

Hvis aftalen mellem dig og en anden part drejer sig om levering af en anden ydelse end behandling af personoplysninger, hvor du ikke har behov for at give eller modtage en instruks om behandling af personoplysninger, vil der ikke være en databehandlingskonstruktion. Dette gælder også, selvom der overleveres nogle personoplysninger (f.eks. navn og adresse), som er nødvendige for at hovedydelsen kan leveres

ROLLER - EKSEMPLER

Dataansvarlig

Håndtering af egne kunderelationer

Databehandler

Hosting

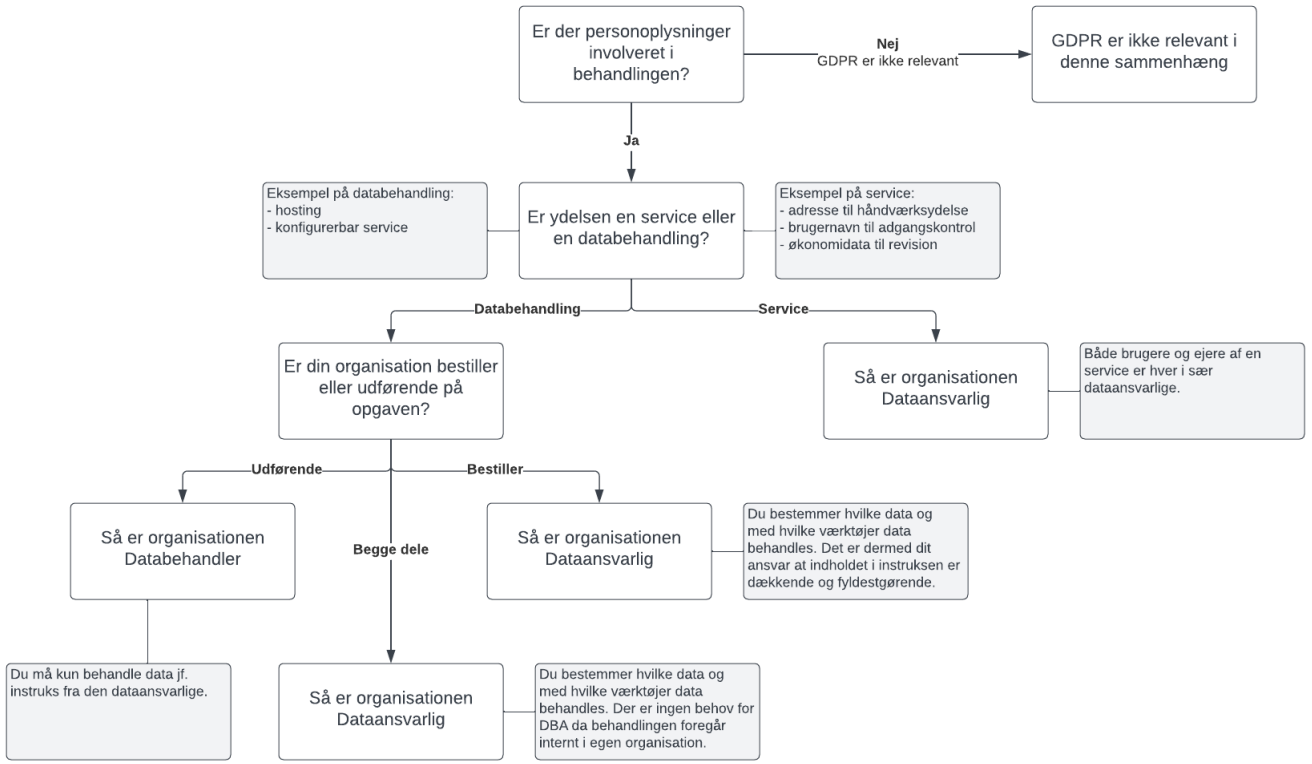
Serviceleverandør

Pensionsrådgivning

BEHANDLINGSAKTIVITETER – DATAANSVARLIG (STANDARD)

Behandlingsaktivitet	Registrerede	Personoplysninger (eksempler)	Ansvarlig (eksempel)
Personaleadministration	Ansatte	Navn, adresse, medarbejder ID, stilling, telefonnummer, fødselsdato, CPR-nummer, bankoplysninger, email, løn, stilling, evt. fagforening, evt. helbredsoplysninger	HR
Rekruttering	Ansøgere	Navn, adresse, email, telefonnummer, fotos, fødselsdag, personlighedstest, stilling, uddannelse - karakterer	HR
Kundeservice	Kunder	(Fra økonomi)	Kundeservice
Fakturering	Kunder	Adresse, betalingsoplysninger, navn, kundenummer, email og telefonnummer	Økonomi

TOMMELFINGERREGLER TIL AFKLARING AF ROLLE



LAKESIDE

STANDARD SERVICES

Som leverandør

- Du skal vurdere om du er Dataansvarlig
  - Er det en take-it-or-leave-it service?
    Fx en betalingsløsning
- eller Databehandler
  - Kan brugerne selv bestemme hvad løsningen skal bruges til, og hvilke data der indsamles?
    Fx en apv-løsning, hvor bruger-organisationen selv opsætter spørgsmål
- I sidste ende er det jeres og jeres kundes egen vurdering
- Standard vilkår
- Standard aftale
- Standard DBA

Som kunde

- Databehandling
  - Du skal vurdere
    - Om der faktisk er tale om en databehandling. Fx hvis der ikke er noget persondata der behandles.
    - Om I kan stå inde for instruksen i standard DBA
- Service – overlevering af data
  - Du skal vurdere
    - Om det data der overføres er rimeligt
    - Om brugen af servicen medfører at data bliver misbrugt eller evt. har konsekvenser for jeres registrerede
- For begge: Brugen af underleverandører

DATAANSVARLIG – ANSVAR OG OPGAVER

a. Ansvarlig for brugen af data
b. Ansvarlig for hvilke data der indsamles, og hvorledes disse behandles og opbevares
c. Ansvarlig for brugen af databehandlere og instruks til databehandling
    a. også selvom databehandleren giver jer en standard DBA!
d. Ansvarlig for tilsyn med databehandlere
e. Ansvarlig for brugen af underdatabehandlere

DATABEHANDLER – ANSVAR OG OPGAVER

a. Overholdelse af dataansvarligs instruks
b. Rådgivning af dataansvarlig ift. informations- og datasikkerhed
c. Understøttelse af dataansvarlig ift. de registreredes rettigheder
d. Understøttelse af dataansvarlig ift. håndtering og rapportering af brud
e. Sikring af ansvarlig brug af evt. underdatabehandlere
    a. også selvom de er godkendt af dataansvarlig
f. Ofte: Tilsyn med underdatabehandlere.

DEN GODE DBA

Den gode databehandleraftale placerer ansvaret de rette steder (rimelig rollefordeling) og sikrer klare aftaler ("let at læse").

OVERORDNET

1. Keep it simple
    1. Brug gerne Datatilsynets standardskabelon
    2. Vær opmærksom på tidsfrister
2. Bilag A – Oplysninger om behandlingen
    1. Scope! Vær præcis
3. Bilag B – Underdatabehandlere
    1. Inkluder kun relevante underdatabehandlere
    2. Ved brug af underleverandører i tredjeland - TIA
4. Bilag C – Instruks vedrørende behandling af personoplysninger
    1. Vælg det rette niveau – beskriv (kort) hvordan hvert krav opfyldes
    2. Fokus: sletteregler!
5. Bilag D – Parternes regulering af andre forhold
    1. Kan fx være en afklaring ift. økonomi ved opgaver som udspringer af DBA.

UNDERDATABEHANDLERE

Afsnit 7 og 8 + Bilag B

1. Hvem kan vælge underdatabehandler?
2. Hvem skal høres?
3. Hvad er orienteringsfristen?
4. Hvem er ansvarlig for udarbejdelse af TIA?
5. Hvem holder tilsyn med underdatabehandlere?

TILSYN

Afsnit 12 + Bilag C afsnit 7 og 8

1. Gør intet med mindre der er noget galt
2. Få en skriftlig bekræftelse på efterlevelse
3. Årlig status på forhold
4. Relevant certificering
5. Revisionserklæring fra tredjepart
6. Du fører selv dokumenteret tilsyn med databehandler

TILSYN

Afsnit 12 + Bilag C afsnit 7 og 8

1. Fastsættelse af tilsynskadance
2. Altid fokus på evt. brud siden sidste tilsyn
3. Kan evt. revisionserklæringer fra underdatabehandlere indgå som dokumentation for overholdelse?
    1. Hvordan?

VÆRKTØJSKATALOG

Der findes virkeligt mange værktøjer derude. Jeg har her samlet lidt af de gratis værktøjer jeg har fundet.

DATATILSYNET - VEJLEDNINGER

- Vejledning til behandling af persondata: https://www.datatilsynet.dk/hvad-siger-reglerne/grundlaeggende-begreber/hvornaar-behandler-du-personoplysninger
- Vejledning til tilsyn med databehandlere: https://www.datatilsynet.dk/Media/637710957381234368/Datatilsynet_Vejledning%20om%20tilsyn%20med%20databehandlere_oktober-2021.pdf
- Vejledning til rollefordeling ved private leverandører til det offentlige: https://www.datatilsynet.dk/Media/637800004810345413/Vejledende%20tekst%20om%20rollefordelingen_2022.pdf
- Vejledning til vurdering af dataansvarlig vs databehandler: https://www.datatilsynet.dk/Media/7/6/Dataansvarlige%20og%20databehandlere.pdf
- Tilstrækkelighedsafgørelse ved overførsel til USA: https://www.datatilsynet.dk/internationalt/internationalt-nyt/2023/jul/eu-kommissionen-vedtager-tilstraekkelighedsafgoerelse-vedroerende-usa
  - Listen over certificerede organisationer: https://www.dataprivacyframework.gov/s/participant-search

GRATIS VÆRKTØJER - (SEMI)OFFENTLIGE

- SMV gratis uddannelse af medarbejdere: https://smv.itta.dk/
- GoLearn via Dansk-IT (gratis for Dansk-IT medlemmer) https://learn.golearn.dk/courses/sikker-it
- D-mærke: https://d-maerket.dk/kom-i-gang/
- Sikker Digital: https://sikkerdigital.dk/virksomhed
  - Minimumskrav myndigheder: https://sikkerdigital.dk/myndighed/tekniske-tiltag/tekniske-minimumskrav/tekniske-minimumskrav-2024

GRATIS VÆRKTØJER - PRIVATE

- Lakeside Datamand: https://www.lakeside.dk/publikationer/datamanden-en-klassifikation-af-data/
- Wired Relations Compliancy flow værktøj (gratis for lille virksomhed - 1 administrator og 150 elementer): https://www.wiredrelations.com/pricing (Dog minus automated vendor management)
- CyperPilot har en del gratis skabeloner: https://www.cyberpilot.io/da/it-sikkerhed-og-gdpr-skabeloner og awareness plakater som man kan downloade
- Cyberday har en del gratis vejledninger og webinarer: https://da.cyberday.ai/academy
- ComplyCloud har en masse guides og hjælpevideoer – det er skrevet af jurister men lettilgængeligt og kræver blot at man registrerer sig på deres side.

Niveau#	Yderst forretningskritiske	Moderat forretningskritiske	Ikke forretningskritiske
4 - Hemmelige			
3 – Skærpet internt fortrolige			
2 - Internt fortrolige			
1 - Delte			
0 - Offentlige			

Mette Thøgersen
Seniorkonsulent
mth@lakeside.dk
Tlf: 26298741

LAKESIDE

KALENDER 2024

NETVÆRKSARRANGEMENTER

XRAY er Lakesides svar på uformelle netværksmøder. Gennem dialog, oplæg og erfaringsudveksling bliver vi klogere på it og digitalisering. XRAY afholdes klokken 14:30 - 17:00 i vores lokaler på Marselisborg Lystbådehavn

21/03	**Sådan griber du it-compliance an** *+ TechCity Aarhus*
06/06	**Roadmapping som proces og strategisk værktøj**
00/09	**Kommer snart**

XRAY
LAKESIDE

EVALUERING

DIN MENING TÆLLER

LAKESIDE


XRAY
LAKESIDE