SKABELONSAMLING

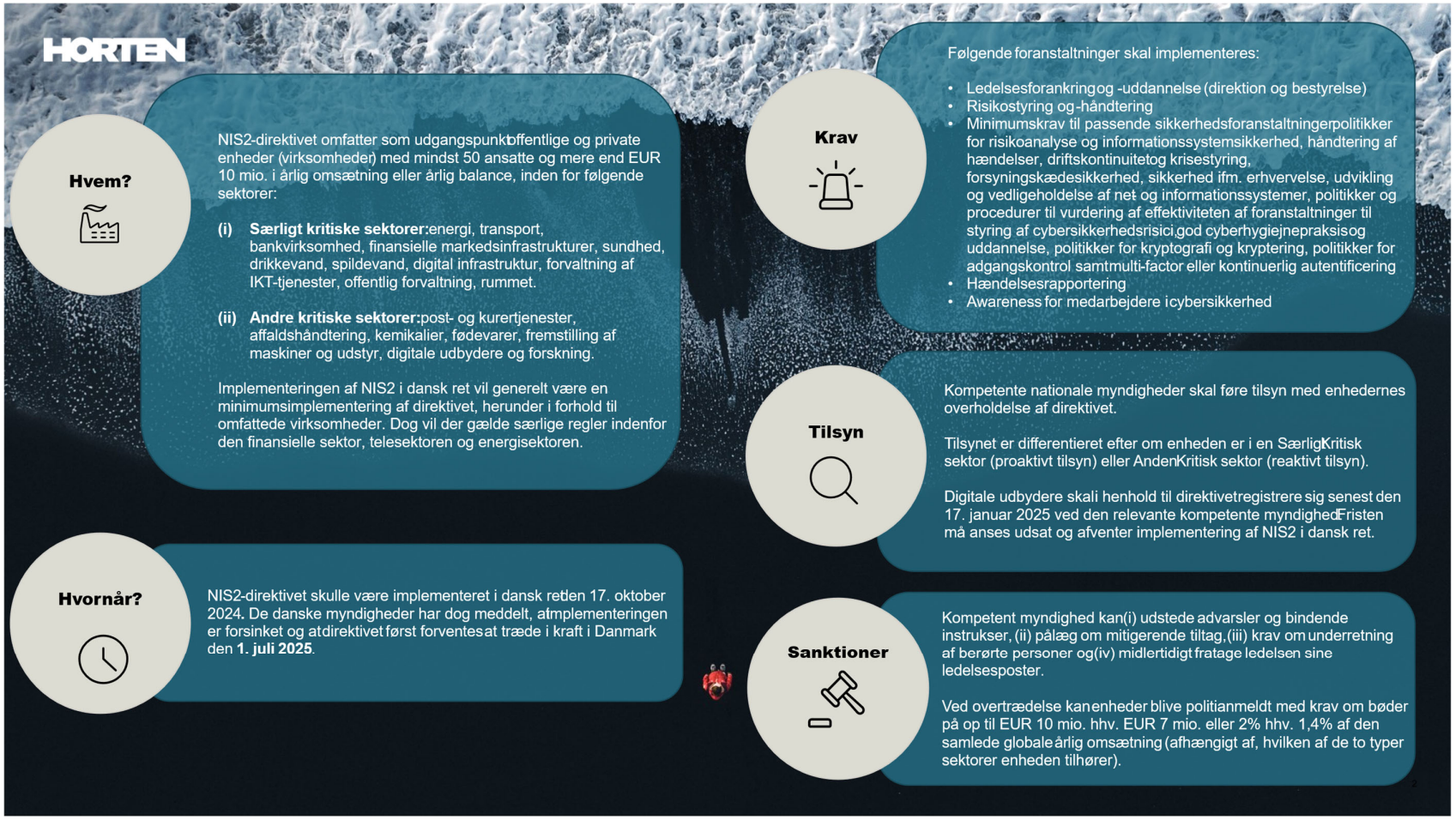
Cyber Safe Robotics

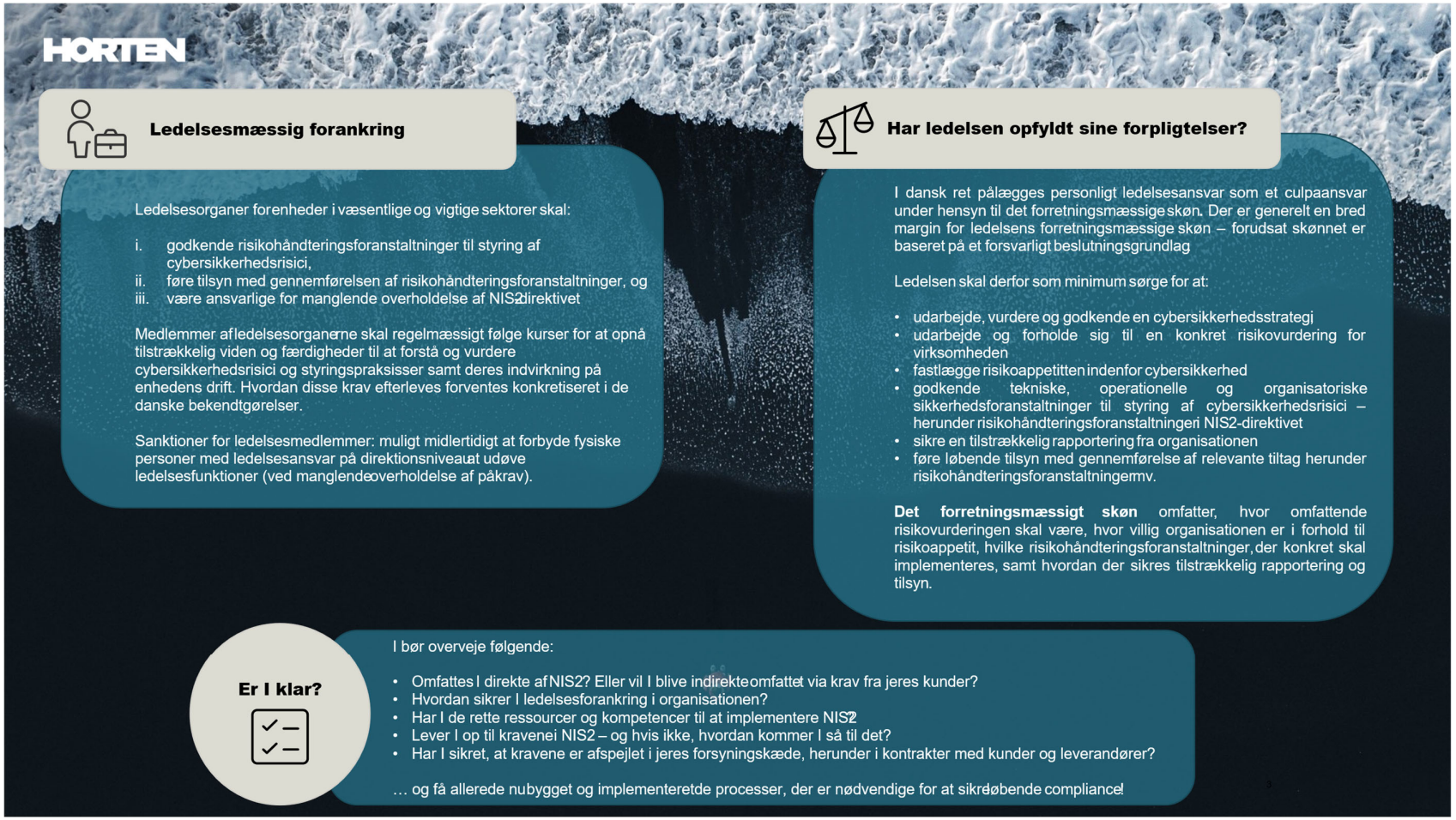
Modul 1 - DET REGULATORISKE LANDSKAB FOR CYBERSIKKERHED

Indhold

1. NIS2 – HAND-OUT....3
2. NIS2 - BESLUTNINGSTRÆ....6
3. RISIKOVURDERING AF IT-SYSTEMER....7
4. RISIKOMATRIX – KLASSIFICERING OG SKALA....9
5. NIS2 - SKABELON FOR KORTLÆGNING AF REGULATORISKE KRAV....14
6. NIS2 - SKABELON FOR IMPLEMENTERINGSPLAN....22
7. CRA – SKABELON FOR KORTLÆGNING AF REGULATORISKE KRAV....26
9. ISO27001 – PROJEKTPLAN....47

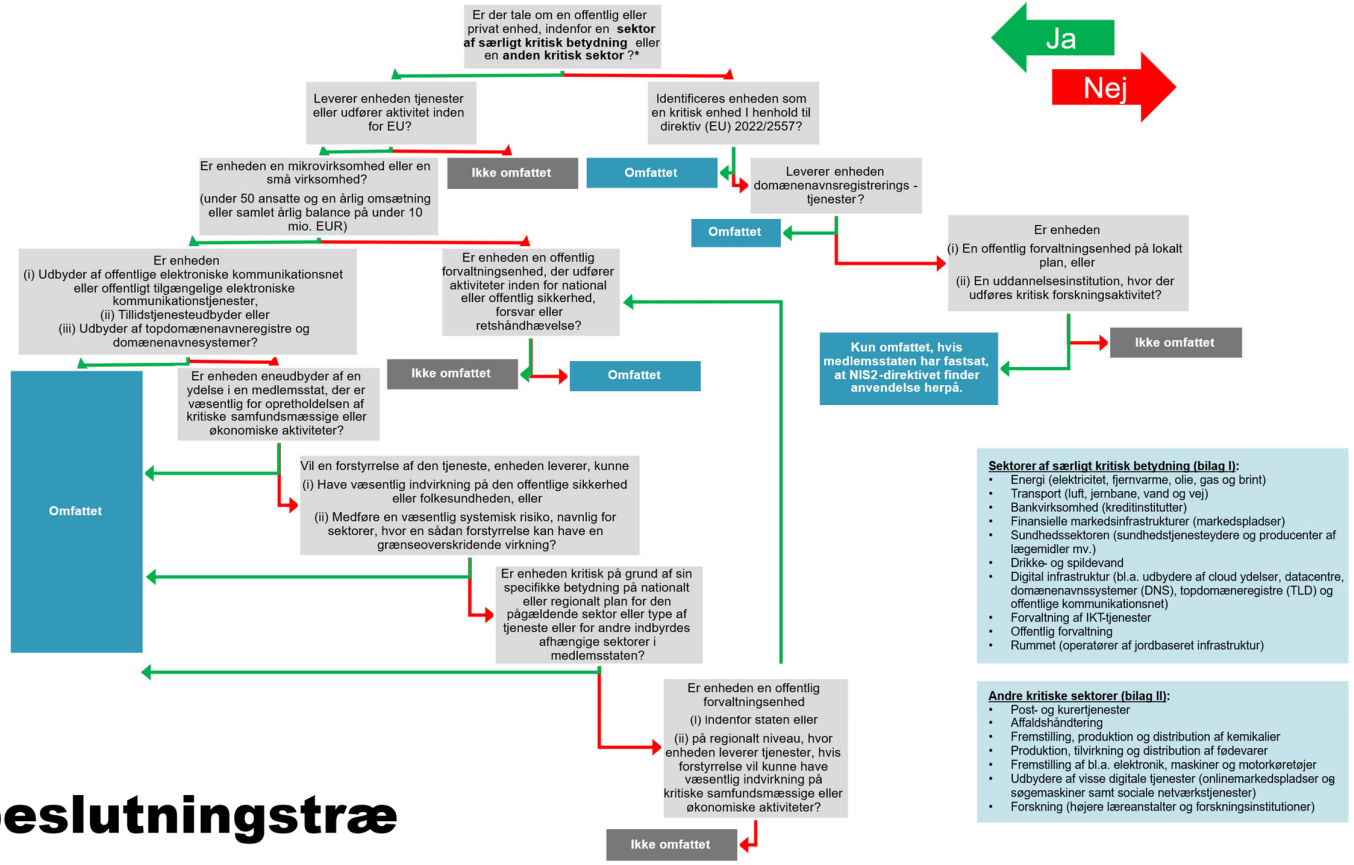
1. NIS2 – HAND-OUT


HORTEN
Hvem?
NIS2-direktivet omfatter som udgangspunkt offentlige og private enheder (virksomheder) med mindst 50 ansatte og mere end EUR 10 mio. i årlig omsætning eller årlig balance, inden for følgende sektorer:
(i) Særligt kritiske sektorer: energi, transport, bankvirksomhed, finansielle markedsinfrastrukturer, sundhed, drikkevand, spildevand, digital infrastruktur, forvaltning af IKT-tjenester, offentlig forvaltning, rummet.
(ii) Andre kritiske sektorer: post- og kurertjenester, affaldshåndtering, kemikalier, fødevarer, fremstilling af maskiner og udstyr, digitale udbydere og forskning.
Implementeringen af NIS2 i dansk ret vil generelt være en minimumsimplementering af direktivet, herunder i forhold til omfattede virksomheder. Dog vil der gælde særlige regler indenfor den finansielle sektor, telesektoren og energisektoren.
Krav
Følgende foranstaltninger skal implementeres:
• Ledelsesforankring og -uddannelse (direktion og bestyrelse)
• Risikostyring og -håndtering
• Minimumskrav til passende sikkerhedsforanstaltninger politikker for risikoanalyse og informationssystemsikkerhed, håndtering af hændelser, driftskontinuitet og krisestyring, forsyningskædesikkerhed, sikkerhed ifm. erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici, god cyberhygiejnepraksis og uddannelse, politikker for kryptografi og kryptering, politikker for adgangskontrol samt multi-factor eller kontinuerlig autentificering
• Hændelsesrapportering
• Awareness for medarbejdere i cybersikkerhed
Tilsyn
Kompetente nationale myndigheder skal føre tilsyn med enhedernes overholdelse af direktivet.
Tilsynet er differentieret efter om enheden er i en Særlig Kritisk sektor (proaktivt tilsyn) eller Anden Kritisk sektor (reaktivt tilsyn).
Digitale udbydere skal henhold til direktivet registrere sig senest den 17. januar 2025 ved den relevante kompetente myndighed. Fristen må anses udsat og afventer implementering af NIS2 i dansk ret.
Hvornår?
NIS2-direktivet skulle være implementeret i dansk ret den 17. oktober 2024. De danske myndigheder har dog meddelt, at implementeringen er forsinket og at direktivet først forventes at træde i kraft i Danmark den 1. juli 2025.
Sanktioner
Kompetent myndighed kan (i) udstede advarsler og bindende instrukser, (ii) pålæg om mitigerende tiltag, (iii) krav om underretning af berørte personer og (iv) midlertidigt fratage ledelsen sine ledelsesposter.
Ved overtrædelse kan enheder blive politianmeldt med krav om bøder på op til EUR 10 mio. hhv. EUR 7 mio. eller 2% hhv. 1,4% af den samlede globale årlig omsætning (afhængigt af, hvilken af de to typer sektorer enheden tilhører).


HORTEN
Ledelsesmæssig forankring
Ledelsesorganer for enheder i væsentlige og vigtige sektorer skal:
i. godkende risikohåndteringsforanstaltninger til styring af cybersikkerhedsrisici,
ii. føre tilsyn med gennemførelsen af risikohåndteringsforanstaltninger, og
iii. være ansvarlige for manglende overholdelse af NIS2-direktivet
Medlemmer af ledelsesorganerne skal regelmæssigt følge kurser for at opnå tilstrækkelig viden og færdigheder til at forstå og vurdere cybersikkerhedsrisici og styringspraksisser samt deres indvirkning på enhedens drift. Hvordan disse krav efterleves forventes konkretiseret i de danske bekendtgørelser.
Sanktioner for ledelsesmedlemmer: muligt midlertidigt at forbyde fysiske personer med ledelsesansvar på direktionsniveau at udøve ledelsesfunktioner (ved manglende overholdelse af påkrav).
Har ledelsen opfyldt sine forpligtelser?
I dansk ret pålægges personligt ledelsesansvar som et culpaansvar under hensyn til det forretningsmæssige skøn. Der er generelt en bred margin for ledelsens forretningsmæssige skøn – forudsat skønnet er baseret på et forsvarligt beslutningsgrundlag
Ledelsen skal derfor som minimum sørge for at:
• udarbejde, vurdere og godkende en cybersikkerhedsstrategi
• udarbejde og forholde sig til en konkret risikovurdering for virksomheden
• fastlægge risikoappetitten indenfor cybersikkerhed
• godkende tekniske, operationelle og organisatoriske sikkerhedsforanstaltninger til styring af cybersikkerhedsrisici – herunder risikohåndteringsforanstaltningerne i NIS2-direktivet
• sikre en tilstrækkelig rapportering fra organisationen
• føre løbende tilsyn med gennemførelse af relevante tiltag herunder risikohåndteringsforanstaltningerne mv.
Det forretningsmæssigt skøn omfatter, hvor omfattende risikovurderingen skal være, hvor villig organisationen er i forhold til risikoappetit, hvilke risikohåndteringsforanstaltninger, der konkret skal implementeres, samt hvordan der sikres tilstrækkelig rapportering og tilsyn.
Er I klar?
I bør overveje følgende:
• Omfattes I direkte af NIS2? Eller vil I blive indirekte omfattet via krav fra jeres kunder?
• Hvordan sikrer I ledelsesforankring i organisationen?
• Har I de rette ressourcer og kompetencer til at implementere NIS2
• Lever I op til kravene i NIS2 – og hvis ikke, hvordan kommer I så til det?
• Har I sikret, at kravene er afspejlet i jeres forsyningskæde, herunder i kontrakter med kunder og leverandører?
… og få allerede nubygget og implementeret de processer, der er nødvendige for at sikre løbende compliance!

2. NIS2 - BESLUTNINGSTRÆ

HORTEN



NIS2-beslutningstræ

3. RISIKOVURDERING AF IT-SYSTEMER

Risikovurdering af IT-system

ID	
Navn (Aktiv/proces)	
Kort beskrivelse	
Risikoejer	

Risikotype	**□ Fortrolighed □ Integritet □ Tilgængelighed**
Risikobeskrivelse	☑
Konsekvens- beskrivelse	
Eksisterende foranstaltninger	
Vurdering	**Sandsynlighed: ___ Konsekvens: ___ Beregnet risiko ___**

Forslag til forbedringer	
Kommentar	
Konklusion	

Udført: Dato og Navn	

Eksempel - Risikovurdering af IT-system

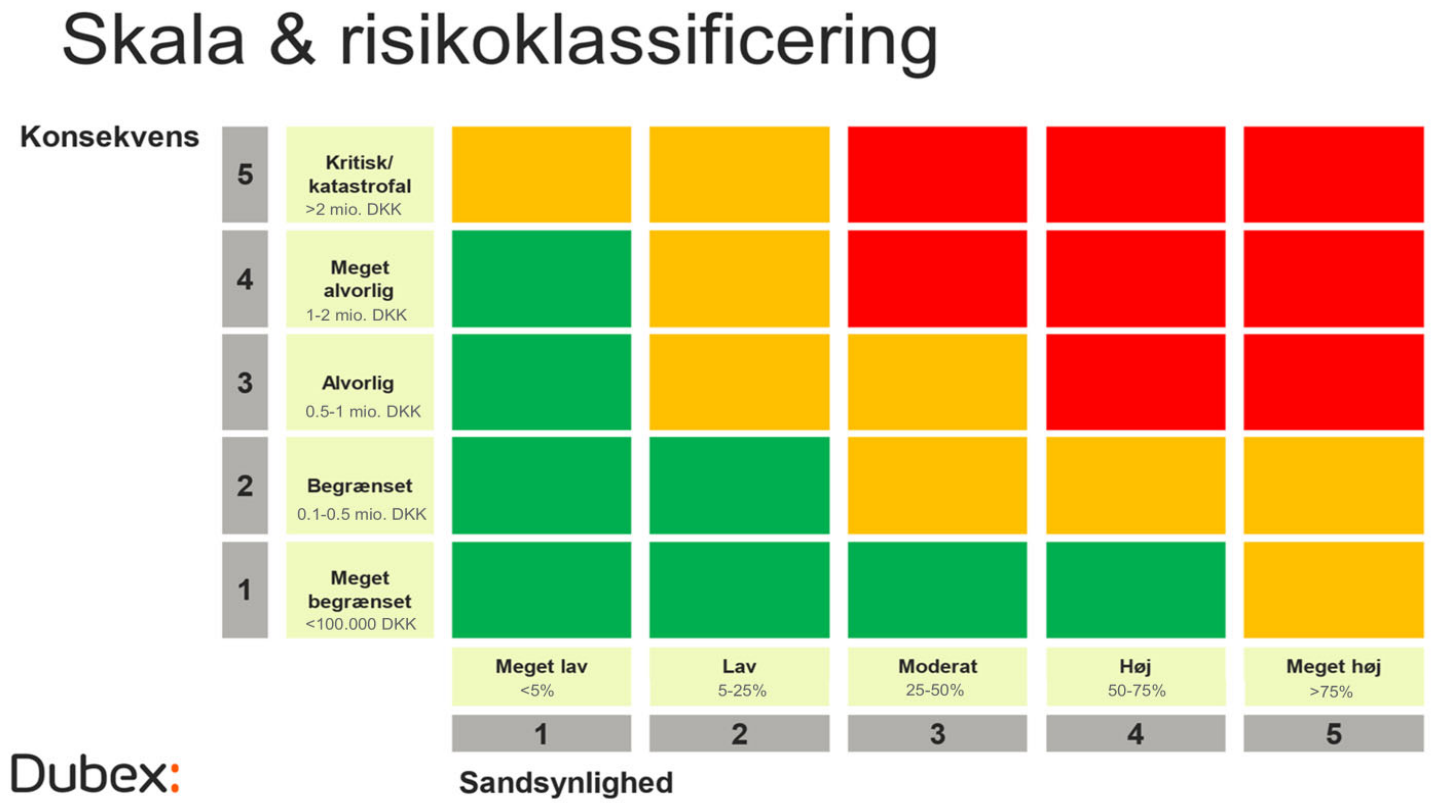
ID	1
Navn (Aktiv/proces)	Hjemmeside
Kort beskrivelse	Virksomhedens hjemmeside der bl.a. bruges til webshop
Risikoejer	Salgsafdelingen

Risikotype	□ **Fortrolighed** □ **Integritet** ☑ **Tilgængelighed**
Risikobeskrivelse	Hjemmesiden udsættes for DDOS angreb DDOS-angreb er blevet mere tilgængelige og mere hyppige
Konsekvens- beskrivelse	Virksomheden kan ikke sælge nogen vare Risiko for at kunderne forsvinder til en anden leverandør
Eksisterende foranstaltninger	Opdateret software Ekstra kapacitet på Internet forbindelse Ekstra kapacitet på servere
Vurdering	**Sandsynlighed: _3_ Konsekvens: _3_ Beregnet risiko _9_**

Forslag til forbedringer	Etablering af cloudløsning til DDoD beskyttelse
Kommentar	
Konklusion	

Udført: **Dato og Navn**	

4. RISIKOMATRIX – KLASSIFICERING OG SKALA



Eksempel på skala for sandsynlighed

Hvor stor er sandsynligheden for at et system er nede, informationer forvanskes eller fortroligheden brydes?

Værdi		Trusler	Modforanstaltninger	Målinger	
		Ustabil HW og SW Underdimensionerede anlæg. Virusangreb, Phishing, Ukyndige brugere. Netværksudstyr uden nødstrøm	Afprøvet SW Driftssikker HW Stabilt net Veluddannet driftspersonale. Redundans	Hvor mange gange har systemet været nede det sidste år?	Hvor lang tid har systemet været nede i det forgangne år?
1	Meget lille				Minutter
2	Lille				Timer
3	Middel				Dage
4	Stor				Uger
5	Katastrofalt stor				Måneder

Dubex:

Eksempel på skala for fortrolighed

Hvor store er konsekvenserne hvis **fortroligheden** i systemet brydes, og uvedkommende får adgang til systemets data?

VÆRDI		Eksempler:	
1	Meget lave eller ingen.	Offentlig tilgængelig information	Web
2	Lave	Informationer der ikke er offentlige, men hvor skade ved offentliggørelse er begrænset.	Office-systemer. Intranet.
3	Middel	Informationer hvortil typisk kun medarbejdere og interne personer typisk må have adgang	Journalsystem uden persondata. Økonomisystem. Tilskudssystem.
4	Store	Personhenførbare eller følsomme informationer	Personalesystemer, f.eks. løn.
5	Katastrofale	Kun udvalgte personer må have adgang, og hvor skade ved andres uvedkommende adgang kan være stor eller katastrofal.	Hemmelige informationer, special-systemer, kan have afgørende økonomiske eller personlige konsekvenser.

Dubex:

Eksempel på skala for integritet

Hvor store er konsekvenserne, når/hvis brugere handler ud fra forkerte eller upålidelige oplysninger?

VÆRDI		Eksempler:
1	Meget lave	Åbningstider eller telefonnr er forkerte. Web-systemer.
2	Lave	Fejlbehæftede e-mails.
3	Middel	Ind- og udbetalinger, lønoverførsler for mellemstore grupper. Økonomisystem.
4	Store	F.eks. fejlagtig planlægning af ressourcer. Fejlindkøb, fejlinvesteringer. Ufuldstændige rapporter, eller søgeresultater (f.eks. ESDH systemer).
5	Katastrofale	Økonomiske data, renteniveau, instruktioner ifm miljøberedskab, sundhedspåvirkende.

Dubex:

Eksempel på skala for tilgængelighed

Hvor store er konsekvenserne for organisationen, hvis systemet er nede eller på anden måde utilgængeligt?

VÆRDI		Eksempler:	Parametre med indflydelse		
			Tålt nedetid	Genetableringstid	Antal brugere
1	Meget lave	Printer ude af drift.	Måneder	Minutter	Få
2	Lave	Økonomisystem.	Uger	Timer	
3	Middel	Lønsystem	Dage	Dage	
4	Store	Office systemer, ESDH.	Timer	Uger	
5	Katastrofale	Samfundskritiske miljøberedskabssystemer	Minutter	Måneder	Mange brugere.

Dubex:

5. NIS2 - SKABELON FOR KORTLÆGNING AF REGULATORISKE KRAV

VÆRKTØJER TIL BRUG FOR NIS2 IMPLEMENTERING

Ved fastlæggelse af om en enhed er omfatte af NIS2 og hvilke krav der skal overholdes samt udarbejdelse af implementeringsplan anvendes følgende procestrin (eventuelt værktøj er angivet i parentes):

- Fastlæggelse af om enheden er omfattet af NIS2 (Beslutningstræ).
- Overblik over it-systemer
- Risikovurdering
- Kortlægning af regulatoriske krav (Skabelon for kortlægning af regulatoriske krav)
- Udarbejdelse af Implementeringsplan, herunder tidsplan (Skabelon for implementeringsplan og tidsplan)

NIS2 - SKABELON FOR KORTLÆGNING AF REGULATORISKE KRAV

Krav i NIS2		
LEDELSESFORANKRING		
Organisatorisk ledelsesforankring	BESKRIVELSE: *Implementering af tiltag der sikrer fornøden ledelsesforankring til understøttelse af et tilstrækkeligt sikkerhedsniveau i overensstemmelse med NIS2.*	
	Eksempler på foranstaltninger: 1. *Organisering, herunder fordeling af roller og ansvar* 2. Indarbejdelse i forretningsorden, dagsordener til ledelsesmøder m.v. el.lign.	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
AWARENESS		
Cybersikkerhedsuddannelse (art. 20, stk. 2 og art. 21 (2)(g))	BESKRIVELSE: *Foranstaltninger skal omfatte cybersikkerhedsuddannelse af ledelsesorganer og medarbejdere, så de kan understøtte opfyldelse af kravene i NIS2.*	
	Eksempler på foranstaltninger: 1. *Planlagt årlig undervisning i cybersikkerhed med direktion og bestyrelse v. ekstern konsulent.* 2. *IT-sikkerhed har 1½ times undervisning ved introdage for nye medarbejdere.* 3. *E-learning (under kontinuerlig udvikling).*	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]

Implementeringsplan

Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
RISIKOSTYRING (proaktivt fokus)		
Politikker for risikoanalyse og informationssystemsikkerhed (art. 21 (2)(a))	BESKRIVELSE: *Der skal udarbejdes en eller flere skriftlige politikker og procedurer for analyse af risici og for informationssikkerhed i enhedens it-systemer.*	
	Eksempler på foranstaltninger: 1. *Valg af informationssikkerhedsstandard (ISO27002) for krav til It-sikkerhedsstyring i underliggende forretningsgange og IT-risikostyringsstandard (ISO27005).* 2. *Udarbejdelse af forretningsgange i samarbejde med relevante afdelinger i organisationen.*	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer (art. 21 (2)(e))	BESKRIVELSE: *Der skal udarbejdes krav, kriterier og proces for indkøb, udvikling og vedligeholdelse af relevante it-systemer.*	
	Eksempler på foranstaltninger: 1. *Forretningsgang for anskaffelser, udvikling og vedligehold af IT-systemer.* 2. *(For anskaffelser) – Etablering af fast IT-kontraktboard m. IT-sikkerhed, IT-drift. Outsourcingansvarlig, DPO, Compliance, Risikostyringsfunktion m. løbende møder.* 3. *(for udvikling og vedligehold) – sikre udviklingsprincipper baseret på best-practice implementeres i eksisterende værktøjer.*	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]

Implementeringsplan

Implementeringsplan

Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver (art. 21 (2)(i))	BESKRIVELSE: *Der skal udarbejdes en eller flere skriftlige politikker og procedurer for personale sikkerhed, adgangskontrol og forvaltning af aktiver.*	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering (art. 21 (2)(h))	BESKRIVELSE: *Der skal udarbejdes en eller flere skriftlige politikker og procedurer for kryptografi og kryptering.*	
	Eksempler på foranstaltninger: 1. *Forretningsgang for minimum niveau af kryptografiske protokoller der skal benyttes (jf. eksisterende kendskab til brudte krypteringer).* 2. *Afstem minimumskrypteringsniveau med IT-leverandør*	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
RISIKOHÅNDTERING (reaktivt fokus)		
Håndtering af hændelser (art. 21 (2)(b))	BESKRIVELSE: *Der skal udarbejdes forretningsgange for håndtering af cybersikkerhedshændelser, herunder kategorisering af kritikalitet m.v.*	
	Eksempler på foranstaltninger: 1. *Forretningsgang for hændelseshåndtering.*	

Implementeringsplan

Implementeringsplan

Implementeringsplan

	2. *Afklaring af specifikt hvornår noget er en hændelse (incident), større hændelse (major incident) og beredskabshændelse.*	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe, og krisestyring (art. 21 (2)(c))	BESKRIVELSE: *Der skal etableres foranstaltninger der understøtter og sikrer driftskontinuitet, herunder styringsredskaber (politikker m.v.) og konkrete tiltag til genetablering.*	
	Eksempler på foranstaltninger: 1. *Forretningsgang for IT-beredskab.* 2. *IT-beredskabsplan som har flere faste dele: Kriterier for aktivering, organisation, fast mødeprocedurer og dagsordner, deaktiveringskriterier, ikke-netværksforbundet kommunikationskanaler.*	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
FORSYNINGSKÆDESIKKERHED		
forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere (art. 21 (2)(d))	BESKRIVELSE: *Implementering af relevante cybersikkerhedskrav overfor enhedens leverandører, herunder under hensyntagen til krav fra enhedens kunder.*	
	Eksempler på foranstaltninger: 1. *Allerede eksisterende leverandør-forums styrket med fokus på forsyningssikkerhed ved kritisk vigtige leverandører.*	

Implementeringsplan

Implementeringsplan

	2. Skal en potentiel leverandør understøtte en kritisk eller vigtig forretningsfunktion, så minimumskrav om revisionserklæringer og/eller audit.	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
REVIEW		
Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici (art. 21 (2)(f))	BESKRIVELSE: *Udarbejdelse af ramme for måling af effektivitet af implementerede cybersikkerhedsforanstaltninger.*	
	Eksempler på foranstaltninger: *1. Forretningsgang for IT-risikostyring* *2. Årlig gennemgang af alle IT-aktiver med alle stabe, kritikalitetsvurdering og koblinger til andre IT-aktiver.* *3. Minimum årlig afrapportering direkte til direktion og bestyrelse i relation til IT-risikostyringsrammeværket og nye / accepterede IT-risici.* *4. Ca. månedlig deltagelse på direktionsmøde* *5. Systemunderstøttelse (for at komme uden om uendelig excel-ark).*	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
RAPPORTERING OG UNDERRETNING		
Procedure og format for rapportering og underretning i tilfælde af informationssikkerhedshændelser	BESKRIVELSE:	

Implementeringsplan

Implementeringsplan

Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
UDVEKSLING AF OPLYSNINGER OM CYBERSIKKERHEDSHÆNDELSER		
Procedure for udveksling af cybrsikkerhedsoplysninger med myndigheder (art. 29)	BESKRIVELSE: *Der skal udarbejdes en eller flere skriftlige politikker og procedurer for udveksling af cybersikkerhedsoplysninger med myndigheder.*	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
KONKRETE SIKKERHEDSFORANSTALTNINGER		
Grundlæggende cyberhygiejnepraksisser (art. 21 (2)(g))	BESKRIVELSE: *Implementering af relevante foranstaltninger til sikring af almindelig god cyberhygiejne i hele organisationen.*	
	Eksempler på foranstaltninger: 1. *Valg af informationssikkerhedsstandard (ISO27002) for krav til It-sikkerhedsstyring i underliggende forretningsgange og IT-risikostyringsstandard (ISO27005).* 2. *Udarbejdelse af forretningsgange i samarbejde med relevante afdelinger i banken.*	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]

Implementeringsplan

Implementeringsplan

Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt i enheden, hvor det er relevant (art. 21 (2)(j))	BESKRIVELSE: *Identificering af relevant behov for multifaktorautentificering og implementering.*	
	Eksempler på foranstaltninger: 1. *VPN always-on MFA (minimumskrav).* 2. *Mange strikse Conditional Access regler.* 3. *Privileged Identity Management (korte tidsrammer for høje privilegier)* 4. *SSO, hvor det giver mening.*	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]

Implementeringsplan

Implementeringsplan

6. NIS2 - SKABELON FOR IMPLEMENTERINGSPLAN

VÆRKTØJER TIL BRUG FOR NIS2 IMPLEMENTERING

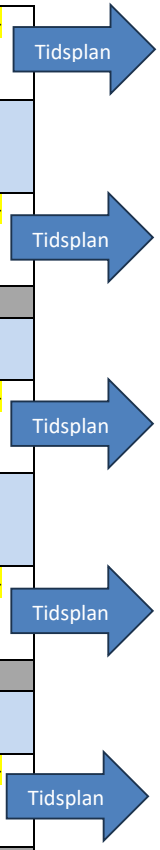
Ved fastlæggelse af om en enhed er omfatte af NIS2 og hvilke krav der skal overholdes samt udarbejdelse af implementeringsplan anvendes følgende procestrin (eventuelt værktøj er angivet i parentes):

- Fastlæggelse af om enheden er omfattet af NIS2 (Beslutningstræ).
- Overblik over it-systemer
- Risikovurdering
- Kortlægning af regulatoriske krav (Skabelon for kortlægning af regulatoriske krav)
- Udarbejdelse af Implementeringsplan, herunder tidsplan (Skabelon for implementeringsplan og tidsplan)

NIS2 - SKABELON FOR IMPLEMENTERINGSPLAN

Krav i NIS2			
LEDELSESFORANKRING			
Organisatorisk ledelsesforankring	Foranstaltninger der skal implementeres:		
[Navn på foranstaltning]	[Standard og reference]	[Beskrivelse af foranstaltning, forudsætninger og kriterie for godkendt implementering]	Tidsplan
AWARENESS			
Cybersikkerhedsuddannelse (art. 21 (2)(g))	BESKRIVELSE:		
[Navn på foranstaltning]	[Standard og reference]	[Beskrivelse af foranstaltning, forudsætninger og kriterie for godkendt implementering]	Tidsplan
RISIKOSTYRING (proaktivt fokus)			
Politikker for risikoanalyse og informationssystemsikkerhed (art. 21 (2)(a))	BESKRIVELSE: *Der skal udarbejdes en eller flere skriftlige politikker og procedurer for analyse af risici og for informationssikkerhed i enhedens it-systemer.*		
[Navn på foranstaltning]	[Standard og reference]	[Beskrivelse af foranstaltning, forudsætninger og kriterie for godkendt implementering]	Tidsplan
Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer (art. 21 (2)(e))	BESKRIVELSE:		
[Navn på foranstaltning]	[Standard og reference]	[Beskrivelse af foranstaltning, forudsætninger og kriterie for godkendt implementering]	Tidsplan
Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver (art. 21 (2)(i))	BESKRIVELSE:		

[Navn på foranstaltning]	[Standard og reference]	[Beskrivelse af foranstaltning, forudsætninger og kriterie for godkendt implementering]
Politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering (art. 21 (2)(h))	BESKRIVELSE:	
[Navn på foranstaltning]	[Standard og reference]	[Beskrivelse af foranstaltning, forudsætninger og kriterie for godkendt implementering]
RISIKOHÅNDTERING (reaktivt fokus)		
Håndtering af hændelser (art. 21 (2)(b))	BESKRIVELSE:	
[Navn på foranstaltning]	[Standard og reference]	[Beskrivelse af foranstaltning, forudsætninger og kriterie for godkendt implementering]
Driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe, og krise-styring (art. 21 (2)(c))	BESKRIVELSE:	
[Navn på foranstaltning]	[Standard og reference]	[Beskrivelse af foranstaltning, forudsætninger og kriterie for godkendt implementering]
FORSYNINGSKÆDESIKKERHED (art. 21 (2)(d))		
Informationssystemsikkerhed hos leverandører	BESKRIVELSE:	
[Navn på foranstaltning]	[Standard og reference]	[Beskrivelse af foranstaltning, forudsætninger og kriterie for godkendt implementering]
REVIEW		
politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici (art. 21 (2)(f))	BESKRIVELSE:	



[Navn på foranstaltning]	[Standard og reference]	[Beskrivelse af foranstaltning, forudsætninger og kriterie for godkendt implementering]
RAPPORTERING OG UNDERRETNING		
Procedure og format for rapportering og underretning i tilfælde af informationssikkerhedshændelser	BESKRIVELSE:	
[Navn på foranstaltning]	[Standard og reference]	[Beskrivelse af foranstaltning, forudsætninger og kriterie for godkendt implementering]
UDVEKSLING AF OPLYSNINGER OM CYBERSIKKERHEDSHÆNDELSER		
Procedure for udveksling af oplysninger med myndigheder	BESKRIVELSE:	
[Navn på foranstaltning]	[Standard og reference]	[Beskrivelse af foranstaltning, forudsætninger og kriterie for godkendt implementering]
KONKRETE SIKKERHEDSFORANSTALTNINGER		
Grundlæggende cyberhygiejnepraksisser (art. 21 (2)(g))	BESKRIVELSE:	
[Navn på foranstaltning]	[Standard og reference]	[Beskrivelse af foranstaltning, forudsætninger og kriterie for godkendt implementering]
Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt i enheden, hvor det er relevant (art. 21 (2)(j))	BESKRIVELSE:	
[Navn på foranstaltning]	[Standard og reference]	[Beskrivelse af foranstaltning, forudsætninger og kriterie for godkendt implementering]

Tidsplan

Tidsplan

Tidsplan

Tidsplan

Tidsplan

8. CYBER RESILIENCE ACT (CRA) - SKABELON FOR KORTLÆGNING AF REGULATORISKE KRAV

CYBER RESILIENCE ACT - SKABELON FOR KORTLÆGNING AF REGULATORISKE KRAV

Krav i CRA		
FABRIKANTENS FORPLIGTELSER IFT. SIKKERHEDSKRAV VED PRODUKTER MED DIGITALE ELEMENTER		
Som fabrikant af produkter med digitale elementer skal man sikre at det er designet, udviklet og produceret i overensstemmelse på en måde som sikrer passende cybersikkerhedsniveau, uden kendte sårbarheder og hvor relevant iagttage sikkerhedskrav i bilag 1, pkt. 1, (3), litra a-k baseret på foretaget risikovurdering	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Produkter med digitale elementer skal leveres med standardsikkerhedsindstilling, herunder muligheden for at nulstille produktet til dets oprindelige tilstand (bilag 1, pkt. 1, (3), litra a)	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]

Implementeringsplan

Implementeringsplan

Produkter med digitale elementer skal sikre beskyttelse mod uautoriseret adgang ved hjælp af passende kontrolmekanismer, herunder, men ikke begrænset til, autentificerings-, identitets- eller adgangsstyringssystemer (bilag 1, pkt. 1, (3), litra b)	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Produkter med digitale elementer skal beskytte fortroligheden af opbevarede, videresendte eller på anden måde behandlede personoplysninger eller andre data, f.eks. ved at kryptere relevante data i hvile eller i transit ved brug af avancerede mekanismer (bilag 1, pkt. 1, (3), litra c)	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Produkter med digitale elementer skal beskytte integriteten af opbevarede, videresendte eller på anden måde behandlede personoplysninger eller andre data, kommandoer, programmer og konfigurationer mod enhver manipulation eller ændring,	BESKRIVELSE:	

Implementeringsplan

Implementeringsplan

som brugeren ikke har givet tilladelse til, samt give melding om korruption (bilag 1, pkt. 1, (3), litra d)		
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Produkter med digitale elementer skal kun behandle personoplysninger eller andre data, der er tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold produktets tilsigtede anvendelse ("dataminimering") (bilag 1, pkt. 1, (3), litra e)	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Produkter med digitale elementer skal beskytte tilgængeligheden af væsentlige funktioner, herunder modstandsdygtighed over for og afbødning af overbelastningsangreb ("denial of service"-angreb) (bilag 1, pkt. 1, (3), litra f)	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]

Implementeringsplan

Implementeringsplan

Implementeringsplan

Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Produkter med digitale elementer skal minimere deres egen negative indvirkning på tilgængeligheden af tjenester, der leveres af enheder eller netværk (bilag 1, pkt. 1, (3), litra g)	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Produkter med digitale elementer skal designes, udvikles og produceres med henblik på at begrænse angrebsflader, herunder eksterne grænseflader (bilag 1, pkt. 1, (3), litra h)	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Produkter med digitale elementer skal designes, udvikles og produceres med henblik på at mindske virkningen af en hændelse ved hjælp af passende mekanismer og teknikker til begrænsning af udnyttelsen (bilag 1, pkt. 1, (3), litra i)	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]

Implementeringsplan

Implementeringsplan

Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Produkter med digitale elementer skal levere sikkerhedsrelaterede oplysninger ved at registrere og/eller overvåge relevante interne aktiviteter, herunder adgang til eller ændring af data, tjenester eller funktioner (bilag 1, pkt. 1, (3), litra j)		
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Produkter med digitale elementer skal sikre, at sårbarheder kan afhjælpes gennem sikkerhedsopdateringer, herunder, hvor det er relevant, gennem automatiske opdateringer og underretning til brugerne om tilgængelige opdateringer. (bilag 1, art. 1, (3), litra k)	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
FABRIKANTENS HÅNDTERING AF SÅRBARHEDER I PRODUKTER MED DIGITALE ELEMENTER		

Implementeringsplan

Implementeringsplan

Implementeringsplan

Fabrikanten skal sikre at produkter med digitale elementers sårbarheder håndteres effektivt og i overensstemmelse med kravene i bilag 1, pkt. 2,(1-8)	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Fabrikanter af produkter med digitale elementer skal identificere og dokumentere sårbarheder og komponenter i produktet, herunder ved at udarbejde en softwarekomponentliste i et almindeligt anvendt og maskinlæsbart format, der som minimum dækker de vigtigste produktafhængigheder (bilag 1, pkt. 2, (1))	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Fabrikanter af produkter med digitale elementer skal i forbindelse med risiciene forbundet med produkter med digitale elementer straks håndtere og afhjælpe sårbarheder, herunder ved at sørge for sikkerhedsopdateringer (bilag 1, pkt. 2, (2))	BESKRIVELSE:	

Implementeringsplan

Implementeringsplan

Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Fabrikanter af produkter med digitale elementer skal regelmæssigt afprøve og gennemgå sikkerheden af produktet med digitale elementer (bilag 1, pkt. 2, (3))	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Fabrikanter af produkter med digitale elementer skal når en sikkerhedsopdatering er gjort tilgængelig, offentliggøre oplysninger om afhjulpne sårbarheder, herunder en beskrivelse af sårbarhederne, oplysninger, der gør det muligt for brugerne at identificere det berørte produkt med digitale elementer, sårbarhedernes indvirkning og alvor og oplysninger, der gør det lettere for brugerne at afhjælpe sårbarhederne (bilag 1, pkt. 2, (4))	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]

Implementeringsplan

Implementeringsplan

Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Fabrikanter af produkter med digitale elementer skal indføre og håndhæve en politik for koordineret offentliggørelse af sårbarheder (bilag 1, pkt. 2, (5))	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Fabrikanter af produkter med digitale elementer skal træffe foranstaltninger til at lette udvekslingen af oplysninger om potentielle sårbarheder i deres produkt med digitale elementer samt i tredjepartskomponenter indeholdt i det pågældende produkt, herunder ved at anføre en kontaktadresse til indberetning af de sårbarheder, der opdages i produktet med digitale elementer (bilag 1, pkt. 2, (6))	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Fabrikanter af produkter med digitale elementer skal sørge for mekanismer til sikker distribution af opdateringer for produkter med digitale elementer for at sikre,	BESKRIVELSE:	

Implementeringsplan

Implementeringsplan

Implementeringsplan

at sårbarheder, der kan udnyttes, afhjælpes eller afbødes rettidigt (bilag 1, pkt. 2, (7))		
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Fabrikanter af produkter med digitale elementer skal sikre, at tilgængelige sikkerhedsrettelser eller opdateringer til afhjælpning af identificerede sikkerhedsproblemer formidles uden unødigt ophold og gratis sammen med vejledende meddelelser, der giver brugerne de relevante oplysninger, herunder om mulige foranstaltninger, der skal træffes (bilag 1, pkt. 2, (8))	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
FABRIKANTENS UDARBEJDELSE AF TEKSNISK DOKUMENTATION		
Fabrikanten skal udarbejde teknisk dokumentation som skal indeholde alle relevante data om de midler, som anvendes for at sikre, at produktet og de processer, som fabrikanten har indført, opfylder de væsentlige krav i bilag 1. Der er i Bilag V	BESKRIVELSE:	

Implementeringsplan

Implementeringsplan

oplistet minimumskrav til hvilke oplysninger dokumentation skal indeholde. Dokumentationen skal gemmes i ti år efter at produktet er blevet bragt i omsætning.		
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Den tekniske dokumentation skal som minimum indeholde følgende oplysninger hvis relevant ift. produktet: - En generel beskrivelse af produktet med digitale elementer, herunder: (a) dets tilsigtede formål (b) softwareversioner, der påvirker overholdelsen af de væsentlige krav (c) hvis produktet med digitale elementer er et hardwareprodukt, fotografier eller illustrationer af dets eksterne elementer, mærkninger og intern indretning (d) oplysninger og anvisninger til brugeren	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]

Implementeringsplan

Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Den tekniske dokumentation skal som minimum indeholde følgende oplysninger hvis relevant ift. produktet: En beskrivelse af design, udvikling og produktion af produktet og af sårbarhedshåndteringsprocesser, herunder: (a) fuldstændige oplysninger om design og udvikling af produktet med digitale elementer, herunder, hvor det er relevant, tegninger og skemaer og/eller en beskrivelse af systemarkitekturen, der forklarer, hvordan softwarekomponenter bygger på eller indgår i hinanden og integreres i den samlede behandling (b) fuldstændige oplysninger om og specifikationer for de sårbarhedshåndteringsprocesser, som fabrikanten har indført, herunder softwarekomponentlisten, politikken for koordineret offentliggørelse af sårbarheder, dokumentation for angivelse af en kontaktadresse til indberetning af sårbarheder og en beskrivelse af de tekniske løsninger, der er valgt til sikker distribution af opdateringer	BESKRIVELSE:	

Implementeringsplan

(c) fuldstændige oplysninger om og specifikationer for produktions- og overvågningsprocesserne for produktet med digitale elementer og validering af disse processer.		
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Den tekniske dokumentation skal som minimum indeholde følgende oplysninger hvis relevant ift. produktet: En vurdering af de cybersikkerhedsrisici, som produktet med digitale elementer designes, udvikles, produceres, leveres og vedligeholdes til at beskytte imod, jf. denne forordnings artikel 10.	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Den tekniske dokumentation skal som minimum indeholde følgende oplysninger hvis relevant ift. produktet:	BESKRIVELSE:	

Implementeringsplan

Implementeringsplan

En liste over de helt eller delvist anvendte harmoniserede standarder. I tilfælde af delvis anvendelse af harmoniserede standarder, fælles specifikationer eller cybersikkerhedscertificeringer skal den tekniske dokumentation angive, hvilke dele der er anvendt.		
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Den tekniske dokumentation skal som minimum indeholde følgende oplysninger hvis relevant ift. produktet: Rapporter om de prøvninger, der er foretaget for at kontrollere, at produktet og sårbarhedshåndteringsprocesserne opfylder de gældende væsentlige krav i bilag 1, punkt 1 og 2.	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Den tekniske dokumentation skal som minimum indeholde følgende oplysninger hvis relevant ift. produktet:	BESKRIVELSE:	

Implementeringsplan

Implementeringsplan

En kopi af EU-overensstemmelseserklæringen.		
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Den tekniske dokumentation skal som minimum indeholde følgende oplysninger hvis relevant ift. produktet: Hvis det er relevant, softwarekomponentlisten	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
FABRIKATENS OPLYSE BRUGEREN AF PRODUKTER MED DIGITALE ELEMENTER		
Produkter med digitale elementer skal som minimum ledsages af oplysningerne oplistet i bilag 2, (1-9)	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]

Implementeringsplan

Implementeringsplan

Implementeringsplan

Produkter med digitale elementer skal som minimum ledsages af oplysningerne om fabrikantens navn, registrerede firmanavn eller registrerede varemærke og postadresse og e-mailadresse skal fremgå af produktet eller, hvis det ikke er muligt, af emballagen eller af et dokument, der ledsager produktet. (bilag 2, (1))	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Produkter med digitale elementer skal som minimum ledsages af oplysningerne om det kontaktpunkt, hvor oplysninger om produktets cybersikkerhedssårbarheder kan indberettes og modtages. (bilag 2, (2))	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Produkter med digitale elementer skal som minimum ledsages af oplysningerne om Korrekt identifikation af type-, parti-, versions- eller serienummer eller en anden form for angivelse, der gør det muligt at identificere produktet, og de relaterede	BESKRIVELSE:	

Implementeringsplan

Implementeringsplan

anvisninger og oplysninger til brugeren. (bilag 2, (3))		
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Produkter med digitale elementer skal som minimum ledsages af oplysningerne om den tilsigtede anvendelse, herunder det sikkerhedsmiljø, som fabrikanten leverer, samt produktets væsentlige funktioner og oplysninger om sikkerhedsegenskaberne. (bilag 2, (4))	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Produkter med digitale elementer skal som minimum ledsages af oplysningerne om Alle kendte eller forudsigelige omstændigheder i forbindelse med anvendelse af produktet med digitale elementer i overensstemmelse med dets tilsigtede formål eller ved fejlanvendelse, der med rimelighed kan forudses, der kan medføre betydelige cybersikkerhedsrisici. (bilag 2, (5))	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]

Implementeringsplan

Implementeringsplan

Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Produkter med digitale elementer skal som minimum ledsages af oplysningerne om hvis og hvor det er relevant, hvor softwarekomponentlisten kan tilgås. (bilag 2, (6))	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Produkter med digitale elementer skal som minimum ledsages af oplysningerne om hvor det er relevant, den internetadresse, hvor der er adgang til EU-overensstemmelseserklæringen. (bilag 2, (7))	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Produkter med digitale elementer skal som minimum ledsages af oplysningerne om den type tekniske sikkerhedsstøtte, som fabrikanten tilbyder, og indtil hvornår den vil blive ydet, i det mindste hvor	BESKRIVELSE:	

Implementeringsplan

Implementeringsplan

Implementeringsplan

længe brugerne kan forvente at modtage sikkerhedsopdateringer. (bilag 2, (8))		
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
Produkter med digitale elementer skal som minimum ledsages af oplysningerne om Detaljerede anvisninger eller en internetadresse med henvisning til sådanne detaljerede anvisninger og oplysninger om: (a) de nødvendige foranstaltninger ved første ibrugtagning og i hele produktets levetid for at sikre en sikker anvendelse heraf (b) hvordan ændringer af produktet kan påvirke datasikkerheden (c) hvordan sikkerhedsrelevante opdateringer kan installeres (d) sikker nedlukning af produktet, herunder oplysninger om, hvordan brugerdata kan fjernes sikkert (bilag 2, (9))	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]

Implementeringsplan

Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
OVERENSTEMMELSESVURDERINGSPROCEDURER		
Fabrikanten foretager en EU-overensstemmelsesvurdering af produktet med digitale elementer og de processer, som fabrikanten har indført, med henblik på at fastslå, om de væsentlige krav i bilag 1 er opfyldt. Kravene til denne vurdering skærpes afhængig af produktet.	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
IMPORTØRENS FORPLIGTELSE VED AT BRINGE PRODUKTER MED DIGITALE ELEMENTER I OMSÆTNING		
Importøren sikrer, før denne bringer et produkt med digitale elementer i omsætning: (a) at fabrikanten har gennemført den relevante EU- overensstemmelsesvurderingsprocedurer (som skal gemmes i 10 år) (b) at fabrikanten har udarbejdet den tekniske dokumentation (se ovenfor)	BESKRIVELSE:	

Implementeringsplan

Implementeringsplan

(c) at produktet med digitale elementer er forsynet med CE-mærkning og er ledsaget af oplysninger og brugsanvisninger.		
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]
DISTRIBUTØRENS FORPLIGTELSE NÅR PRODUKTER MED DIGITALE ELEMENTER GØRES TILGÆNGELIGE		
Inden et produkt med digitale elementer gøres tilgængeligt på markedet, kontrollerer distributøren, at: (a) produktet med digitale elementer er forsynet med CE-mærkning (b) fabrikanten og importøren har udarbejdet teknisk dokumentation, relevante EU-overensstemmelsesvurdering og har påført produktet importørens navn, registrerede firmanavn eller registrerede varemærke, postadresse og e-mailadresse, eller hvis dette ikke er muligt, af emballagen eller af et dokument, der ledsager produktet.	BESKRIVELSE:	
Implementerede foranstaltninger (as-is)	[Navn]	[Beskrivelse]
Vurderes foranstaltninger helt eller delvist, at være utilstrækkelige henset til gældende risikovurdering?	[Ja]/[Nej]	[Begrundelse]
Foranstaltninger der skal implementeres (to-be)	[Navn]	[Beskrivelse]

Implementeringsplan

Implementeringsplan

9. ISO27001 – PROJEKTPLAN

KUNDENAVN

ISO 27001 PROJEKTPLAN

Følgende er udfyldt som eksempel:

Version:	*1.0*
Dato for version:	*10-11-2024*
Udarbejdet af:	*Jens Jensen*
Godkendt af:	*Mads Madsen*
Klassifikation:	*Fortrolig*

Historik

Følgende er udfyldt som eksempel:

Dato	**Version**	**Udarbejdet af**	**Beskrivelse af ændring**
15-04-2024	*0.1*	*JEJ*	*Første udkast til dokumentet*
02-05-2024	*0.2*	*CHE*	*Kommentarer og rettelser*
11-08-2024	*0.3*	*JEJ*	*Rettelser i dokument*
12-08-2024	*0.4*	*JEJ*	*Sidste rettelser, sendt til godkendelse*
10-11-2024	*1.0*	*MAM*	*Godkendt dokument*

Indholdsfortegnelse

FORMÅL, OMFANG OG BRUGER 49
1. REFERENCE DOKUMENTER 49
2. ISMS INTRODUKTIONSPROJEKT 49
2.1. Projektets formål 49
2.2. Resultater af projektet 49
2.3. Tidsfrister 50
2.4. Projekt organisation 50
2.4.1. Projektejer 50
2.4.2. Projektleder 51
2.4.3. Projekt 51
LISTE OVER PROJEKTDELTAGERE 51
2.5. Vigtigste risici i projektet 51
2.6. Værktøjer til projektimplementering, rapportering 52
3. GYLDIGHED OG DOKUMENTHÅNDTERING 52

Formål, omfang og bruger

Formålet med denne projektplan er klart at beskrive målene for implementeringsprojektet for <Virksomhedsnavns> Information Security Management System (ISMS), de krævede dokumenter, deadlines og roller og ansvar i den forbindelse, samt aktiviteter der skal gennemgås.
Brugere af dette dokument er medlemmer af [ledelsen] og medlemmer af projektteamet.

Reference dokumenter

- ISO/IEC 27001-standard

ISMS introduktionsprojekt

Projektets formål

Projektet har til formål at styrke den interne sikkerhed i <Virksomhedsnavn>, herunder både den tekniske og organisatoriske sikkerhed. Det valgte rammeværk for dette er ISO 27001 og deraf implementering af et ISMS.

Resultater af projektet

Som del af de indledende faser, oprettes følgende dokumenter:

- **Anvendelsesområdet** - et dokument til den nøjagtige definition af værdier (aktiver), placeringer, teknologier mv. inden for anvendelsesområdet
    - **Erklæring om anvendelighed** – Et dokument, der fastlægger formålet med og anvendeligheden af hver foranstaltning i overensstemmelse med bilag A til ISO 27001
- **Procedure for kontrol af dokumentation**– regler for oprettelse, godkendelse, distribution og ajourføring af dokumenter og optegnelser
- **Procedurer for fastlæggelse af krav** – identifikation af lovgivning, regulativer og kontraktuelle forpligtelser
- **Informationssikkerhedsretningslinjer** - et centralt dokument for styring af informationssikkerhed (f.eks. CIA-modellen - Confidentiality, Integrity, Availability)
- **Metode til risikovurdering og risikobehandling** – beskrivelse af metoden til håndtering af informationsrisici
- **Risikovurdering** - Alle dokumenter udarbejdet under risikovurderings- og behandlingsprocessen
    - **Risikovurderingskatalog** - Resultat af vurderingen af værdier, trusler og sårbarheder
    - **Risikobehandlingskatalog** – En liste, hvor relevante foranstaltninger vælges for hver uacceptabel risiko
    - **Risikobehandlingsplan** – Beskriver de handlinger der skal gennemføres for at nedbringe identificerede risici, inkluderer frister og ressourcer der skal afsættes.
- **Interne revisionsprocedurer** – beskriver hvordan revisorer udvælges, revisionsprogrammer oprettes, udføres, og logges
- **Procedure for korrigerende handlinger** – beskriver proceduren for gennemførelse af korrigerende og forebyggende foranstaltninger

- **Ledelsesevalueringsreferater** – referat fra ledelsesmødet for at vurdere, om ISMS er tilstrækkeligt

Tidsfrister

Følgende er fristerne for frigivelse af de enkelte dokumenter i løbet af ISMS-introduktionen:

Følgende er udfyldt som eksempel:

Møde uge	***Opfølgning uge***	***Dokument***	***Frist for dokumentfrigivelse***
0-2	4-5	**Procedure for kontrol af dokumentation**	Uge 6
2-4	6-7	**Procedurer for fastlæggelse af krav**	Uge 8
4-6	8-9	**Anvendelsesområdet** **- Erklæring om anvendelighed**	Uge 10
6-8	10-11	**Informationssikkerhedsretningslinje**	Uge 12
8-10	12-13	**Metode til risikovurdering og risikobehandling**	Uge 14
10-12	14-15	**Risikovurdering** - **Risikovurderingskatalog** - **Risikobehandlingskatalog** - **Risikobehandlingsplan**	Uge 16
12-14	16-17	**Interne revisionsprocedurer**	Uge 18
14-16	18-19	**Procedure for korrigerende handlinger**	Uge 20
16-18	20-21	**Ledelsesevalueringsreferater**	Uge 22
18-20	22-23	**Fremadrettet planlægning**	Uge 24

Endelig præsentation af projektresultaterne er planlagt til [dato].

Projekt organisation

Projektejer

Projektejeren deltager ikke aktivt i projektet. Projektejeren skal hver [XXX] informeres af projektlederen om projektstatus. Det er projektejerens ansvar at gribe ind hvis projektet skal afbrydes, eller større omstruktureringer skal foretages.

Projektejeren er: [navn, jobtitel]

Projektleder

Projektlederens rolle omfatter følgende opgaver: sikring af de ressourcer, der er nødvendige for projektgennemførelsen, koordinering af projektet, orientering af projektsejer om projektets fremskridt, udførelse af administrative opgaver i forbindelse med projektet.

Projektlederens beføjelser bør sikre projektgennemførelsen uden afbrydelser inden for de fastsatte frister.

Projektlederen er: [Navn, titel]

Projekt

Projektteamets rolle omfatter følgende opgaver: støtte i forskellige aspekter af projektgennemførelsen, udførelsen af definerede opgaver, samt rådgivning til beslutninger om forskellige aspekter, der kræver en tværfaglig tilgang.

Liste over projektdeltagere

Følgende er udfyldt som eksempel:

Navn	***Organisatorisk enhed***	***Stillingsbetegnelse***	***Telefon***	***E-mail***
Anna Jensen	*IT-afdeling*	*IT-sikkerhedsansvarlig*	*614501XX*	*Anna.jensen@virksomhed.dk*
Jens Jensen	*IT-afdeling*	*Senior Risk & Compliance*	*456852XX*	*Jens.Jensen@virksomhed.dk*
Bjørn Hansen	*Juridisk afdeling*	*Juridisk rådgiver*	*879456XX*	*Bjorn.Hansen@virksomhed.dk*
Clara Sørensen	*Finans afdeling*	*Finansanalytiker*	*585526XX*	*Clara.sorensen@virksomhed.dk*
Mads Madsen	*Ledelse*	*Chief Technical Officer*	*468476XX*	*Mads.madsen@virksomhed.dk*

Vigtigste risici i projektet

[Indsæt beskrivelse af de væsentlige risici der ses i forbindelse med projekt, samt hvilke foranstaltninger der er på plads for at hindre det i at ske]

Følgende er udfyldt som eksempel:

Risiko	**Beskrivelse**	**Foranstaltninger**
Manglende ledelsesmæssig støtte	*Hvis ledelsen udviser passende engagement og opbakning, kan det påvirke projektets succes og ressourceallokering negativt.*	*- Regelmæssige møder med ledelsen for at sikre opbakning.* *- Klare kommunikationskanaler og rapportering.*
Tekniske udfordringer	*Implementering af nye sikkerhedsteknologier kan støde på tekniske problemer eller inkompatibilitet.*	*- Grundig teknisk evaluering før implementering.* *- IT-support er til rådighed for at løse problemer*
Tidsplanoverskridelser	*Projektet kan tage længere tid end planlagt, hvilket kan påvirke budget og ressourcer.*	*- Realistisk tidsplanlægning.* *- Løbende overvågning af projektets fremdrift og justering af ressourcer efter behov.*

Værktøjer til projektimplementering, rapportering

[Indsæt beskrivelse om hvor dokumenter der er under udarbejdelse og ikke publiceret, skal opbevares]

Følgende er udfyldt som eksempel:

Opbevaring: *Alle dokumenter, der er under udarbejdelse og ikke publiceret, skal opbevares centralt i SharePoint – Documents -> Internal -> ISO27001 indtil frigivelse.*
Dokumenterne bliver følgende lagt op ved frigivelse på SharePoint – Documents -> Shared -> ISO27001

Adgangskontrol: *Begræns adgangen til dokumenterne til autoriserede projektdeltagere via brugerrettigheder og autentificering.*

Gyldighed og dokumenthåndtering

Dette dokument er gyldigt fra [Dato]
Ejeren af dokumentet er [jobtitel].
Ved evalueringen af dokumentet for effektivitet og tilstrækkelighed skal følgende kriterier tages i betragtning:

- Hvorvidt alle medarbejdere, der er involveret i projektet, udfører deres aktiviteter i henhold til specifikationerne i dette dokument
- Om alle projektfrister overholdes

[Stillingsbetegnelse]
[Navn]

_____
[Underskrift]