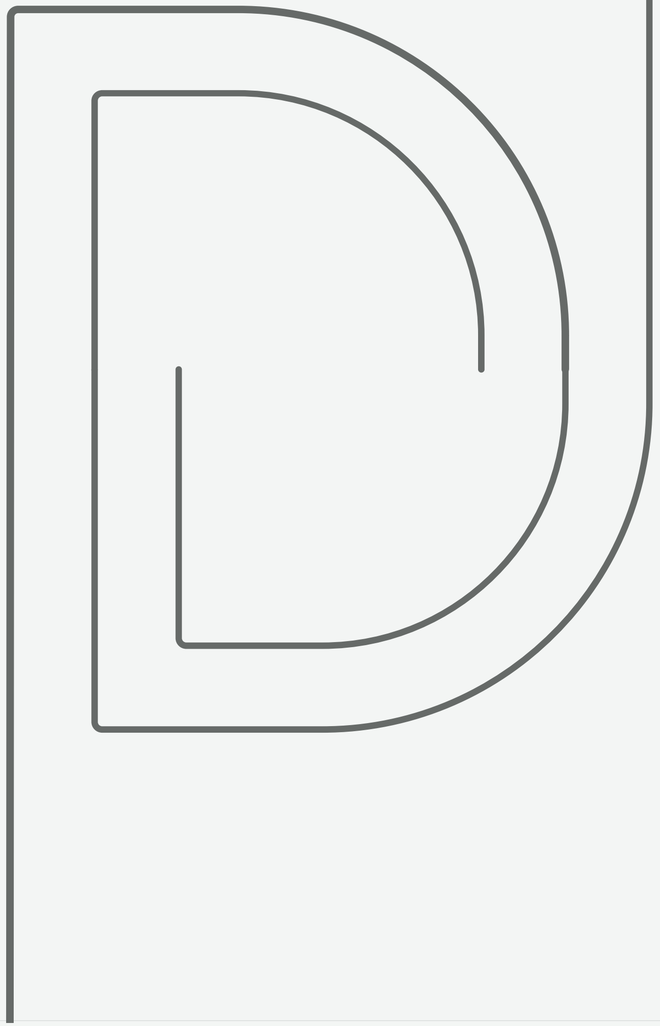
Danmarks nye mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse

Mikael Jensen, D-mærket

DS Cyberdag
D-mærket – sådan kommer du godt i gang

Tid
Torsdag d. 29. september 2022 I 15:25 – 15:55

Sted
Dansk Standard I Göteborg Plads 1 I 2150 Nordhavn



DANSK ERHVERV

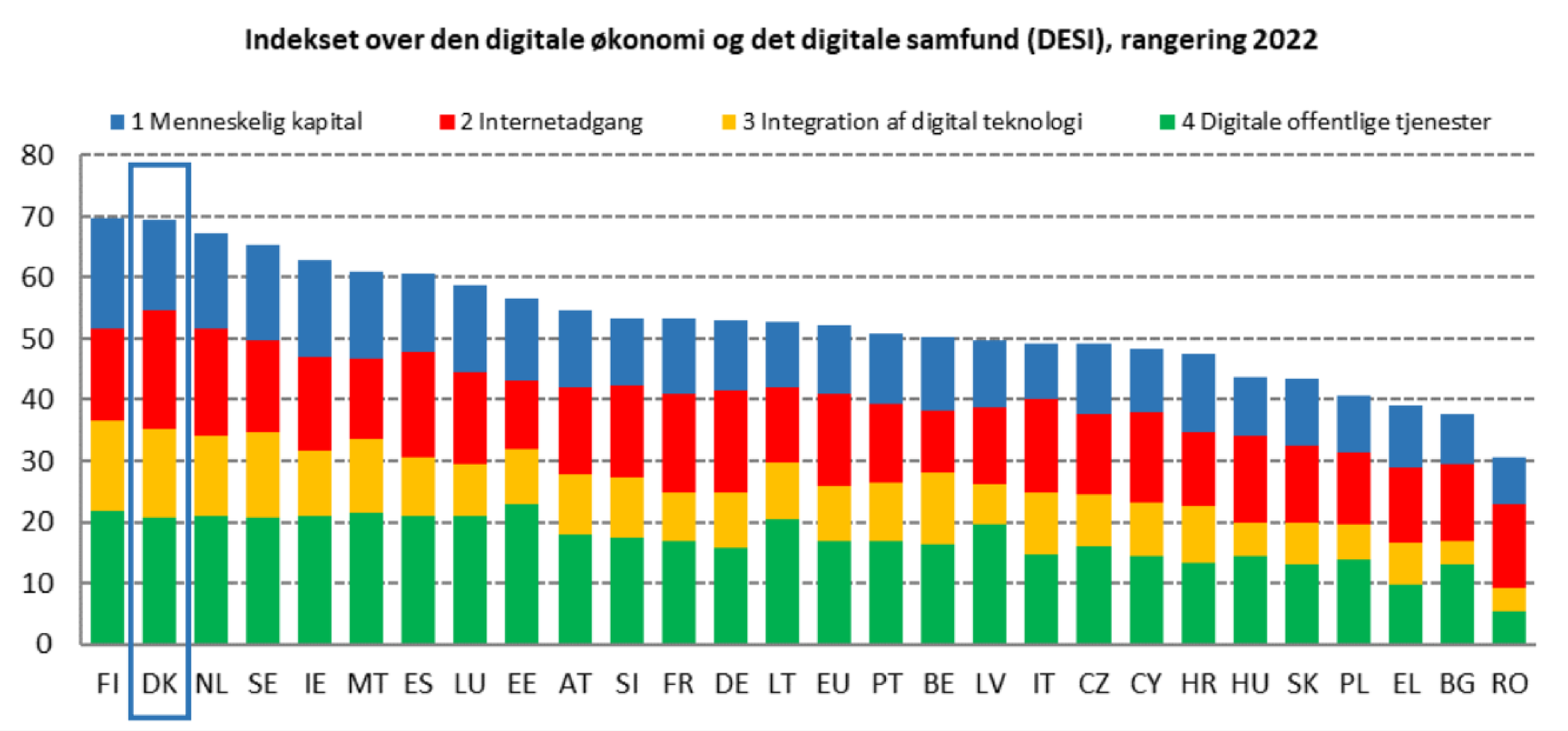
SMVdanmark

FORBRUGERRÅDET tænk

Kapitel 1

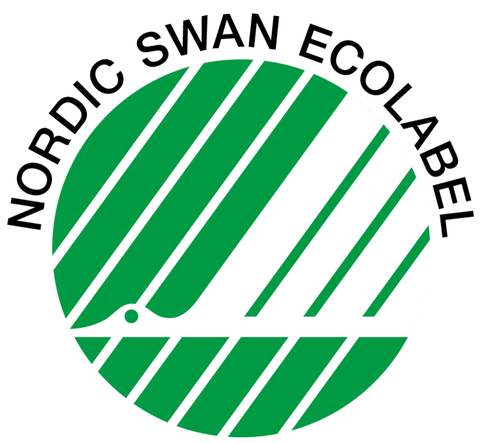
Baggrund og formål

Danmark er ét af de mest digitaliserede lande



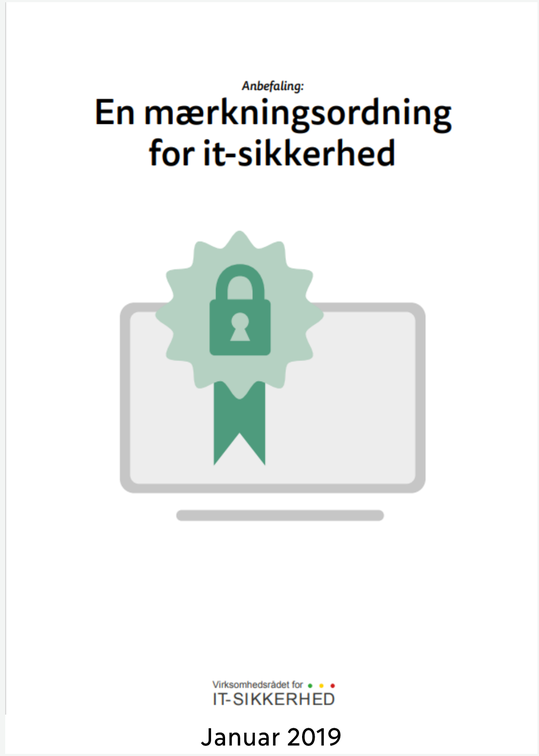
Kilde: The Digital Economy and Society Index — Countries' performance in digitisation | Shaping Europe's digital future (europa.eu)

Der findes mærker indenfor mange områder

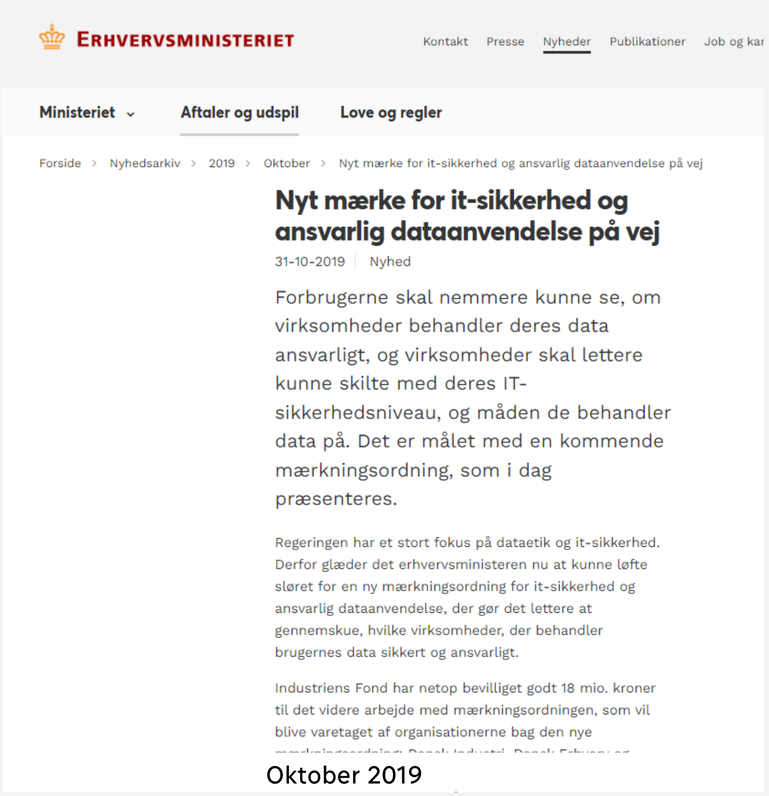


Baggrund for D-mærke-initiativet

November 2018



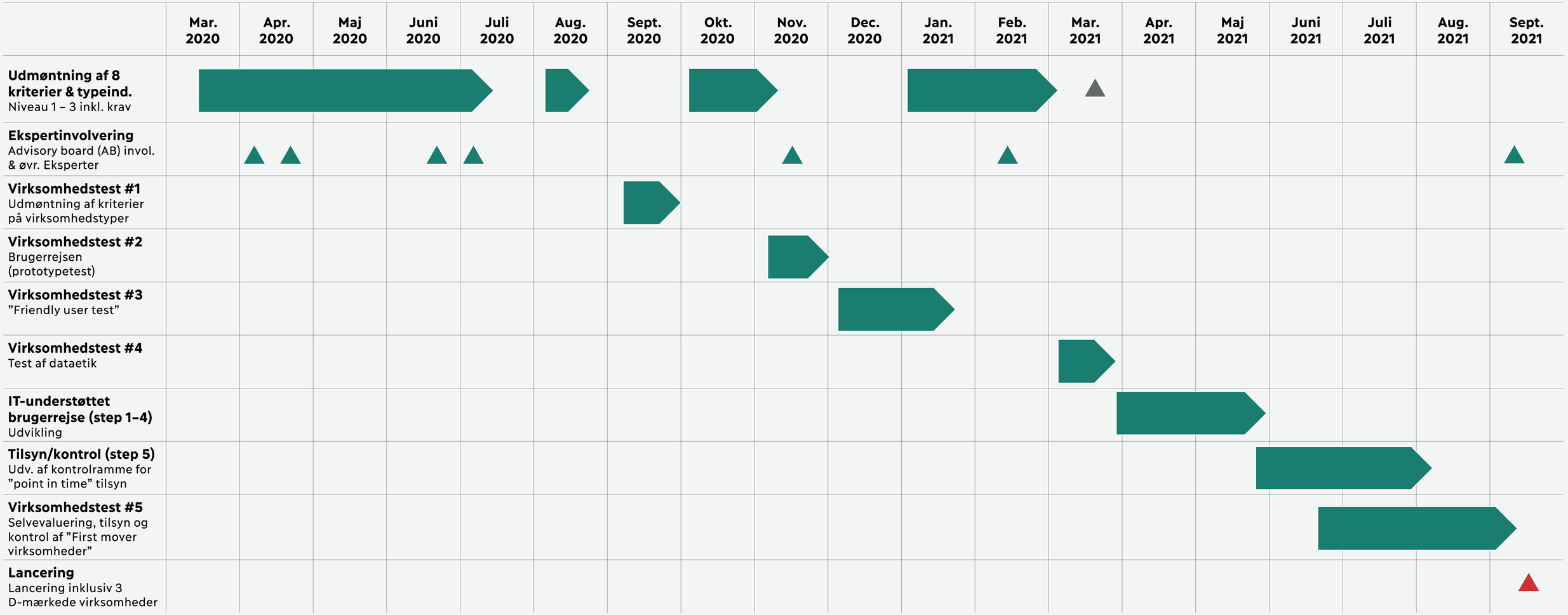
Januar 2019



Oktober 2019

Kilde: Regeringens ekspertgruppe klar med anbefalinger om dataetik (em.dk); Virksomhedsrådet for IT-sikkerhed: Danmark skal have et mærke for it-sikkerhed (em.dk); Nyt mærke for it-sikkerhed og ansvarlig dataanvendelse på vej (em.dk)

Det tog halvandet år at gøre D-mærket lanceringsklar



D-mærket blev lanceret den 22. september 2021

PENGE

Nu kan virksomheder skilte med 'D-mærket', hvis de passer godt på dine data

En lang række organisationer står bag D-mærket, der skal øge virksomheders it-sikkerhed og fokus på forbrugernes data.

Kilde: Nu kan virksomheder skilte med 'D-mærket', hvis de passer godt på dine data | Penge | DR

Kendskab til D-mærket ultimo 2021

16%

Kendskab til D-mærket blandt danske SMV'ere

24%

Kendskab til D-mærket blandt "De Digitale" danske SMV'ere

Kilde: Erhvervsstyrelsens kendskabsanalyse for SMV'ere i samarbejde med Epinion, dec. 2021

Status efter første år – september 2022

~500

virksomheder/organisationer i gang med D-mærket

Kilde: D-mærket

Der er et stort potentiale!

Cyber- og informationssikkerheden i danske SMV'er skal styrkes

40 %

af SMV'erne har et utilstrækkeligt digitalt sikkerhedsniveau i forhold til deres risikoprofil.

Kilde: Digital sikkerhed i danske SMV'er, Erhvervsstyrelsen, 2021.

24 %

af de danske SMV'er har ikke implementeret de to helt basale sikkerhedstiltag; opdatering af styresystemer og backup af data.

Kilde: Digital sikkerhed i danske SMV'er, Erhvervsstyrelsen, 2021.

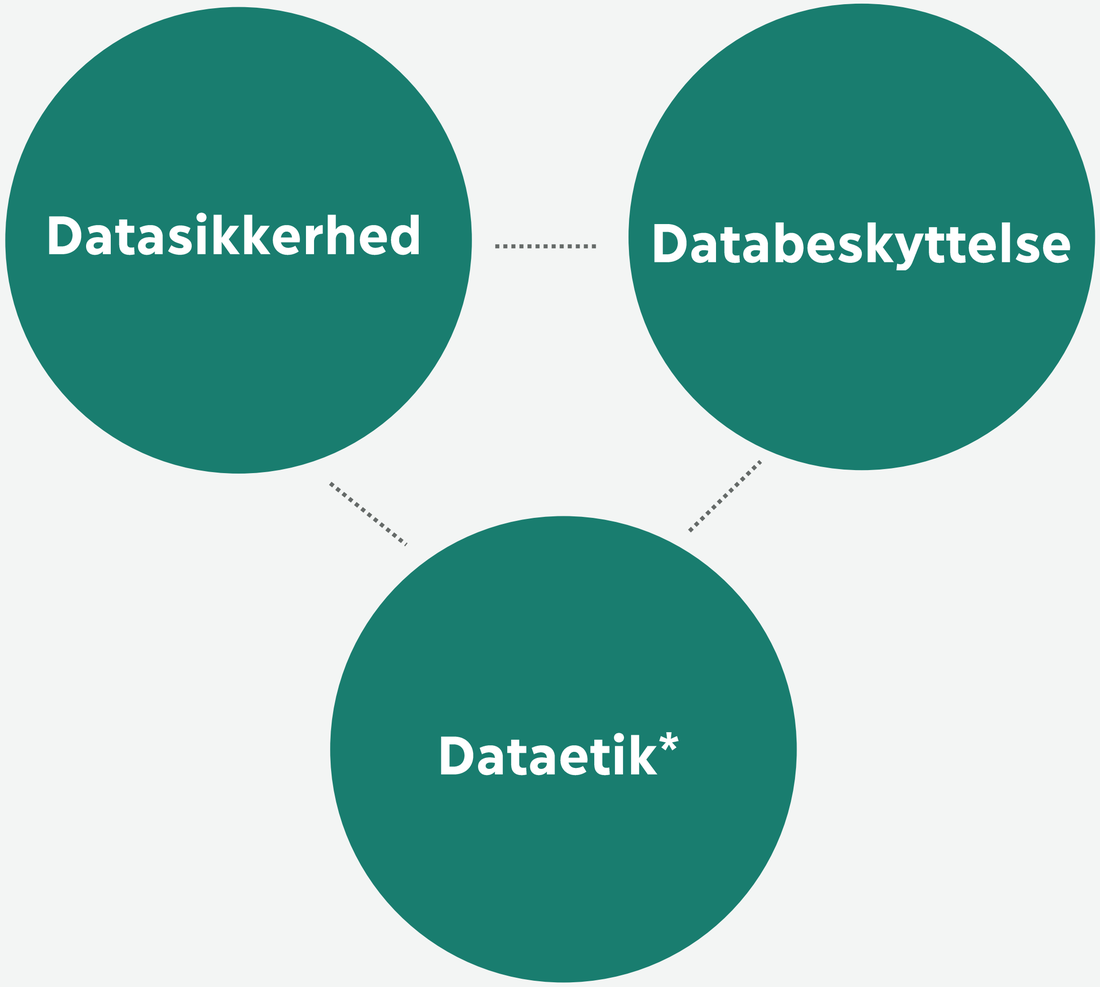
Kilde: Danmarks digitaliserings strategi – sammen om den digitale udvikling, Regeringen, maj 2022

FORMÅL

D-mærket skal skabe digital tryghed hos kunder og forbrugere og digital ansvarlighed hos virksomheder og organisationer ...

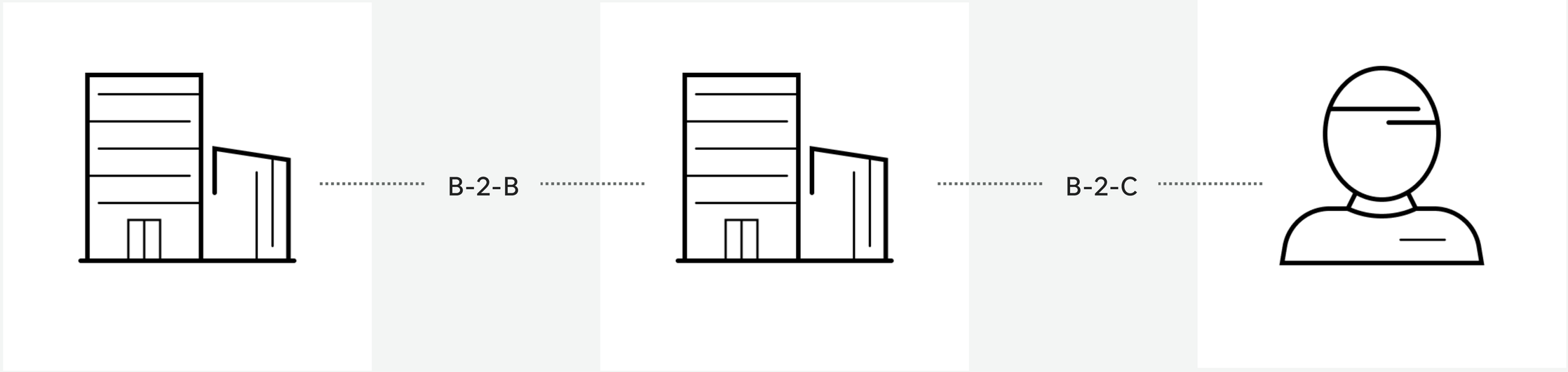
1. **... ved at give dansk erhvervsliv et solidt løft for it-sikkerhed og ansvarlig dataanvendelse**
2. **... ved at give forretningsværdi**
3. **... ved at skabe transparens og tryghed hos kunder og samarbejdspartnere**
4. **... ved at gøre it-sikkerhed og ansvarlig dataanvendelse til en dansk og europæisk styrkeposition**

D-mærkets kriterier omhandler ...



* Inkl. krav til Privacy & Security by Design & Default i softwareudvikling samt krav til pålidelige algoritmer & kunstig intelligens

D-mærket er relevant for alle typer virksomheder



digital tryghed

digital tryghed

digital trust

digital trust

D-MÆRKET

Dubex A/S

Gyldigt: 22.09.2021 – 01.11.2022
D-mærket siden: 22.09.2021

D-mærket - en frivillig mærkningsordning for
it-sikkerhed og ansvarlig dataanvendelse

Virksomhedsoplysninger

Dubex A/S
Gyngemose Parkvej 50
2860 Søborg
CVR: 19556603

Gå til virksomhedens hjemmeside

Dubex:

Gruppe III

KRITERIE 1
Styring og forankring i ledelsen

KRITERIE 2
Awareness og sikker adfærd

KRITERIE 3
Teknisk it-sikkerhed

KRITERIE 4
Krav til leverandørers it-sikkerhed og ansvarlige dataanvendelse

KRITERIE 5
Transparens & kontrol med data

KRITERIE 8
Dataetik

De gældende kriterier og krav for virksomheden afhænger af virksomhedens størrelse, forretningsmodel, brug af data, it og dets indflydelse på mennesker. D-mærket tildeles på baggrund af tilsyn med udvalgte kriterier og krav. Læs om D-mærket på www.d-mærket.dk.

Kilde: Dubex A/S | D-mærket (d-maerket.dk)

D-MÆRKET

ViSikrer ApS

Gyldigt: 20.06.2022 – 01.07.2023
D-mærket siden: 20.06.2022

D-mærket - en frivillig mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse

Virksomhedsoplysninger

ViSikrer ApS
C/O Johnny Dalgaard, Egeparken 3
4862 Guldborg
CVR: 40969861

Gå til virksomhedens hjemmeside

Gruppe I

KRITERIE 1
Styring og forankring i ledelsen

KRITERIE 2
Awareness og sikker adfærd

KRITERIE 3
Teknisk it-sikkerhed

KRITERIE 4
Krav til leverandørers it-sikkerhed og ansvarlige dataanvendelse

KRITERIE 5
Transparens & kontrol med data

De gældende kriterier og krav for virksomheden afhænger af virksomhedens størrelse, forretningsmodel, brug af data, it og dets indflydelse på mennesker. D-mærket tildeles på baggrund af tilsyn med udvalgte kriterier og krav. Læs om D-mærket på www.d-mærket.dk.

Kilde: ViSikrer ApS | D-mærket (d-maerket.dk)

Compliance-, cyber- og tillidstrusler

Databeskyttelse

Compliance trusler

- Personal data breach
  (breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed)

Datasikkerhed

Cybertrusler

- Supply chain threat
- Non-malicious threats
- Cryptojacking
- Disinformation/ Misinformation
- Ransomware
- Threats against data
- Threats against availability & integrity
- Malware
- Email related threats

Dataetik

Tillidstrusler

- Hateful & Criminal Actors
  (e.g., ransomware)
- Implicit Trust & User Understanding
- Truth, Disinformation, Propaganda
  (e.g., video-faking algorithms)
- Machine Ethics & Algorithmic Biases
  (e.g., application of AI in critical domains like welfare, education, employment, and criminal justice)
- Surveillance State
  (e.g., misuse of facial recognition technology)
- Addiction & the Dopamine Economy
  (e.g., misuse of conversation bots)
- Data Control & Monetization
- Economic & Asset Inequalities
  (e.g., driven by misuse of automation)

Kilder: Cybertruslen mod Danmark i lyset af Ruslands invasion af Ukraine; ENISA Threat Landscape 2021; 2018 Institute for the Future and Omidyar Network. (CC BY-NC-SA 4.0). SR-2005 | ethicalOS.org

Omfattende regulering og anseelige konsekvenser ved manglende overholdelse

POLITICO

FROM POLITICOPRO

Instagram fined €405M for violating kids' privacy

The fine is the third for a Meta-owned company handed down by the Irish regulator.

Christophe Simon/AFP via Getty Images

BY VINCENT MANANCOURT

SEPTEMBER 5, 2022 | 4:20 PM

NIS2 nærmer sig: Bøder for sjusk med it-sikkerheden vokser

NIS-direktiv | 23. maj kl. 03:45

Illustration: Morten Kjerumgaard.

Selvom der sidste efterår var udsigt til NIS2-bøder på max 2 og 4 millioner euro, er beløbet vokset i den endelige aftale, fortæller Morten Løkkegaard (V). Han ville ikke risikere, at virksomhederne fravalgte loven, fordi det er billigere at betale en løsesum.

Kilder: Instagram fined €405M for violating kids' privacy – POLITICO (ampproject.org); NIS2 nærmer sig: Bøder for sjusk med it-sikkerheden vokser | Version2

Stigende fokus på digital sikkerhed og ansvarlighed i hele værdikæden

VIRKSOMHEDSCASE

› Hackerangreb gjorde DESMI konkurrencedygtig

Et phishingangreb fik pumpevirksomheden DESMI til yderligere at opruste på deres IT-sikkerhed. Det har vist sig at være en konkurrencefordel i dag, hvor de er længere end deres konkurrenter.

› **Se video og læs mere om DESMI**

Ny afgørelse

Datatilsynet fastholder forbud i Chromebook-sag

Dato: 18-08-2022

Nyhed

I en meget omtalt sag om brug af Google Workspace i Helsingør Kommune har Datatilsynet nu forholdt sig til det materiale, kommunen senest har leveret. På den baggrund fastholder Datatilsynet det forbud, der blev nedlagt i juli.

Datatilsynet fastholder i en ny afgørelse det behandlingsforbud mod Helsingør Kommunes brug af Google Workspace, som tilsynet nedlagde i midten af juli.

Kilder: Hackerangreb gjorde DESMI konkurrencedygtig (sikkerdigital.dk); Datatilsynet fastholder forbud i Chromebook-sag

Stigende politisk fokus på cybersikkerhed og digital ansvarlighed

17.08.2022 | 3 min læsetid

Nyt udspil til styrket cybersikkerhed

IDA har sammen med SF udarbejdet en strategi for, hvordan vi som samfund må og skal investere i cybersikkerhed for at gøre Danmark digitalt sikkert.

af Ole Hoff-Lund

IDA-formand Laura Klitgaard (tv) og SF-formand Pia Olsen Dyhr vil have fart på investeringerne i cybersikkerhed for at beskytte den kritiske infrastruktur i Danmark. Foto: Mikkel Bech-Hansen

Danmark er et af verdens mest digitaliserede lande – men langt fra det mest digitalt sikre land. Det betyder, at alle de fordele, vi som samfund høster ved vores høje grad af digitalisering, samtidig gør os meget sårbare overfor forskellige former for cyberangreb og it-kriminalitet.

IDA

Vejen til et top-cybersikkert Danmark

Denne indsats har tre formål:

1. Bedre beskyttelse af den offentlige sektor.
2. Danmark skal have verdens mest tjekkede private virksomheder.
3. Borgernes viden om it-sikkerhed skal være høj.

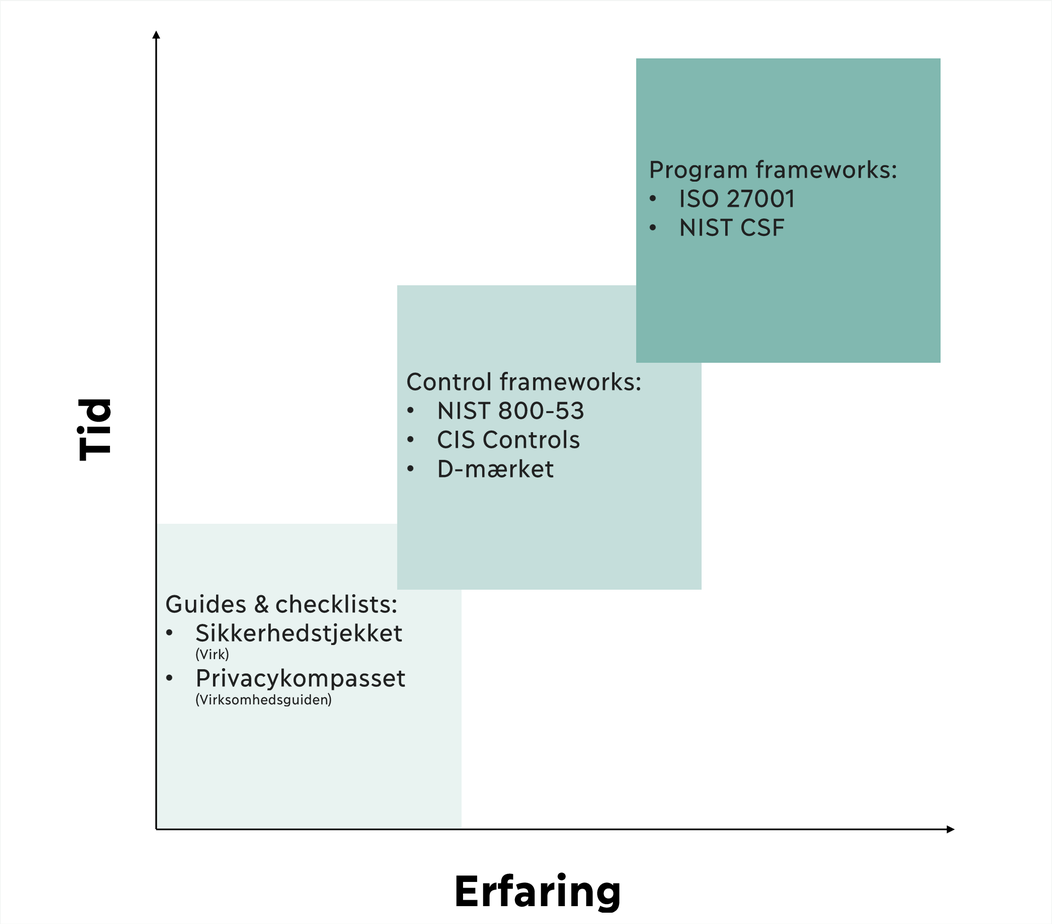
Der er mange gode fem- og tiårsplaner, men nogle gange er man nødt til at handle hurtigt, der hvor man kan det. Der er rigtig mange fordele at hente i at plukke de lavthængende frugter - vi giver her vores bud på, hvad der kan gøres på bare tre måneder, hvis vi vil det. Det er dog på ingen måder nok. Et tilpas cybersikkerhedsniveau kræver dybere spadestik og har mere realistisk et tre-års sigte. Endelig er der grundlæggende forandringer, som tager tid. Men meget bør alligevel kunne nås på 6 år.

Kilde: Nyt udspil til styrket cybersikkerhed fra IDA og SF | IDA; https://ida.dk/media/11383/cyberudspil.pdf

Kapitel 2

Hvad er D-mærket?

Kompleksitet i it-sikkerhedsarbejdsmetoder i forhold til en SMV's modenhed



Inspired by: "Anbefaling: En mærkningsordning for it-sikkerhed", Virksomhedsrådet for IT-sikkerhed (December 2018) & CIS Controls V7 poster https://www.cisecurity.org/white-papers/cis-controls-v7-poster/

Hvilken gruppe tilhører din virksomhed?

Antallet af kriterier og krav som virksomheden skal leve op til afhænger af virksomhedsgruppen, men alle virksomheder skal som minimum leve op til kriterie 1, 2, 3 og 5.

Kriterier for indplacering i gruppe	Gruppe I	Gruppe II	Gruppe III	Gruppe IV
Antal ansatte	0-9	10-49	50-249	250+
Nettoomsætning (mio. DKK)	0-7,9	8-155,9	156-313	≥ 313
Leverandør af software eller it-tjenester	Nej	Nej	Ja	Ja
Behandler særlige kategorier af personoplysninger (fx helbredsoplysninger, race, sexualitet)	Nej	Ja	Ja	Ja

Kilde: https://d-maerket.dk/virksomhedsgrupper/

D-mærkets 8 kriterier

1
KRITERIE 1
Styring og forankring i ledelsen

2
KRITERIE 2
Awareness og sikker adfærd

3
KRITERIE 3
Teknisk it-sikkerhed

4
KRITERIE 4
Krav til leverandørers it-sikkerhed og ansvarlige dataanvendelse

5
KRITERIE 5
Transparens & kontrol med data

6
KRITERIE 6
Privacy & security by design & default

7
KRITERIE 7
Pålidelige algoritmer & AI

8
KRITERIE 8
Dataetik

Kilde: https://d-maerket.dk/kriterier/

Oversigt over D-mærkets kriterier på niveau 1 og 2 samt relation til rammeværker

KRITERIE 1 Styring og forankring i ledelsen	KRITERIE 2 Awareness og sikker adfærd	KRITERIE 3 Teknisk it-sikkerhed	KRITERIE 4 Krav til leverandørers it-sikkerhed og ansvarlige dataanvendelse	KRITERIE 5 Transparens & kontrol med data	KRITERIE 6 Privacy & security by design & default	KRITERIE 7 Pålidelige algoritmer & AI	KRITERIE 8 Dataetik
NIVEAU 2 KRITERIER 1.1 Roller og ansvar i forhold til it-sikkerhed og ansvarlig dataanvendelse 1.2 Overblik over data og systemer 1.3 Risikostyring 1.4 Politik for it-sikkerhed 1.5 It-beredskabsplan 1.6 Politikker for ansvarlig dataanvendelse 1.7 Udviklingsproces	NIVEAU 2 KRITERIER 2.1 Træn bestyrelsen og den øverste ledelse i sikkerhed, databeskyttelse og dataetik 2.2 Awareness om og træning i it-sikkerhed 2.3 Awareness om og træning i ansvarlig dataanvendelse	NIVEAU 2 KRITERIER 3.1 Netværkssikkerhed og kryptering 3.2 Korrekt konfiguration 3.3 Beskyttelse af administrative brugerkonti 3.4 Beskyttelse mod malware 3.5 Kontinuerlig opdatering af software og styresystemer 3.6 Beskyttelse mod tab af vigtige og fortrolige data 3.7 Overvågning af systemaktivitet gennem logning	NIVEAU 2 KRITERIER 4.1 Leverandørlivscyklus og risikovurdering 4.2 Krav til it-sikkerhed hos leverandører 4.3 Krav til ansvarlig databehandling hos leverandører	NIVEAU 2 KRITERIER 5.1 Information i relation til personoplysninger 5.2 Cookies 5.3 Kontrol over egne personoplysninger 5.4 Lettilgængelig klagevejledning	NIVEAU 2 KRITERIER 6.1 Vurdering 6.2 Privacy by design & default 6.3 Security by design & default 6.4 Implementering igennem udviklingsproces	NIVEAU 2 KRITERIER 7.1 Menneskeligt tilsyn og mellemkomst/indgriben og transparens 7.2 Data- og modelkvalitet 7.3 Implementering igennem udviklingsproces	NIVEAU 2 KRITERIER 8.1 Dataetik
EUROPÆISKE KILDER • GDPR	EUROPÆISKE KILDER • GDPR • Europarådet*	EUROPÆISKE KILDER • GDPR • High-Level Expert Group on AI (EU)	EUROPÆISKE KILDER • GDPR	EUROPÆISKE KILDER • GDPR • Datatilsynet (NO) • Datatilsynet (DK) • ENISA**	EUROPÆISKE KILDER • GDPR • Datatilsynet (NO) • ENISA**	EUROPÆISKE KILDER • GDPR • Council of Europe* • High-Level Expert Group on AI (EU) • AIEI Group (DE) • German Data Ethics Commission (DE) • French Data Protection Authority (CNIL) • DS/PAS 2500–1.2020 (DK) • DS/PAS 2500-2.2020 (DK) • *AI Act (EU)* • *CEN-CENELEC JTC 21 Artificial Intelligence*	EUROPÆISKE KILDER • Den Europæiske Unions charter om grundlæggende rettigheder • Rådet for Digital Sikkerhed (DK) • Dataethics.eu (DK) • Ekspertgruppen om dataetik (DK) • Dataetisk Råd (DK) • UK GOV, Data Ethics Framework (UK) • ICO: Age Appropriate Design Code (UK)
INTERNATIONAL SOURCES • ISO/IEC 27001:2013 • ISO/IEC 27701:2019 • NIST-CSF • CIS Controls	INTERNATIONAL SOURCES • ISO/IEC 27001:2013 • ISO/IEC 27701:2019 • NIST-CSF • CIS Controls	INTERNATIONAL SOURCES • ISO/IEC 27001:2013 • ISO/IEC 27701:2019 • NIST-CSF • CIS Controls • OECD recommendations on AI	INTERNATIONAL SOURCES • ISO/IEC 27001:2013 • ISO/IEC 27701:2019 • NIST-CSF • CIS Controls	INTERNATIONAL SOURCES • ISO/IEC 27001:2013 • ISO/IEC 27701:2019	INTERNATIONAL SOURCES • ISO/IEC 27001:2013 • ISO/IEC 27701:2019	INTERNATIONAL SOURCES • OECD recommendations on AI • *ISO/IEC JTC1/SC42 Artificial Intelligence* (Standardization in the area of Artificial Intelligence)	INTERNATIONAL SOURCES • Ethical OS (US)

* Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems
** Privacy and Data Protection by Design–from policy to engineering

Kapitel 3

Hvordan kommer din virksomhed i gang?

Proces for virksomheder

1 **Registrering**

2 **Indplacering og kriterier**

3 **Selvevaluering**

4 **Anmodning og betaling**

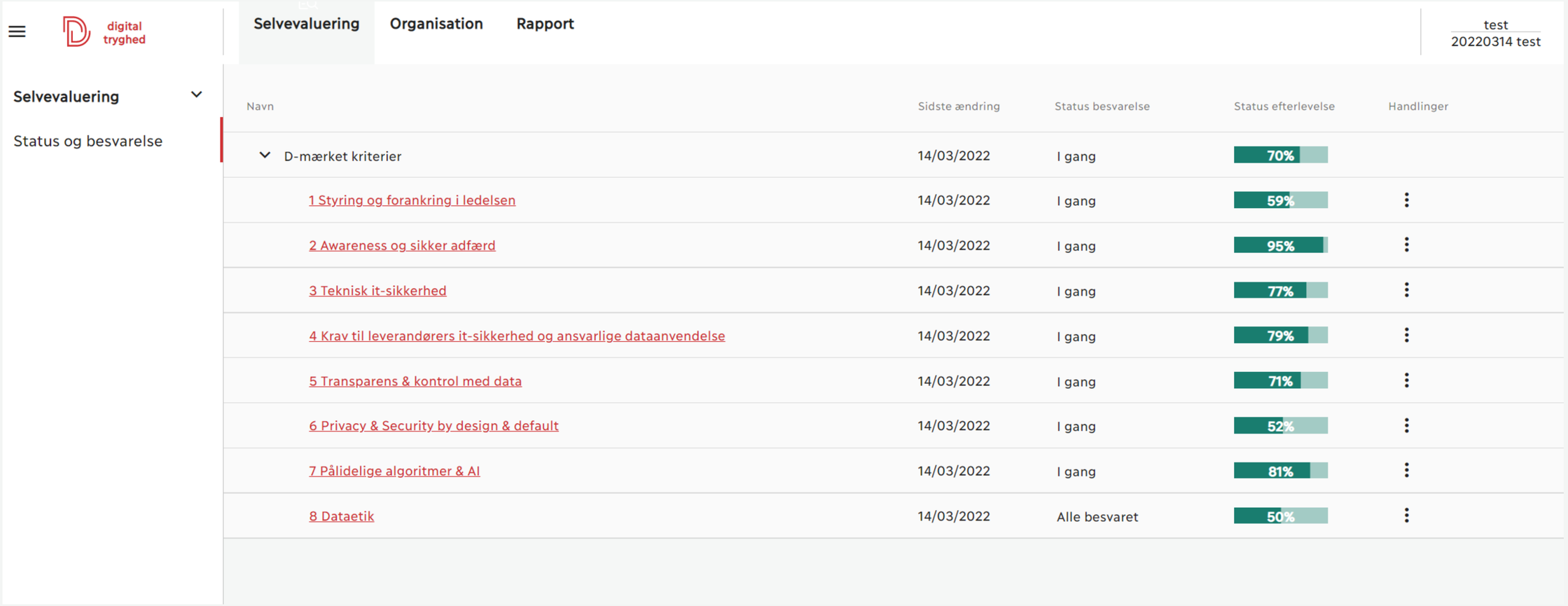
5 **Tilsyn og kontrol**

6 **Tildeling af D-mærke**

Gratis

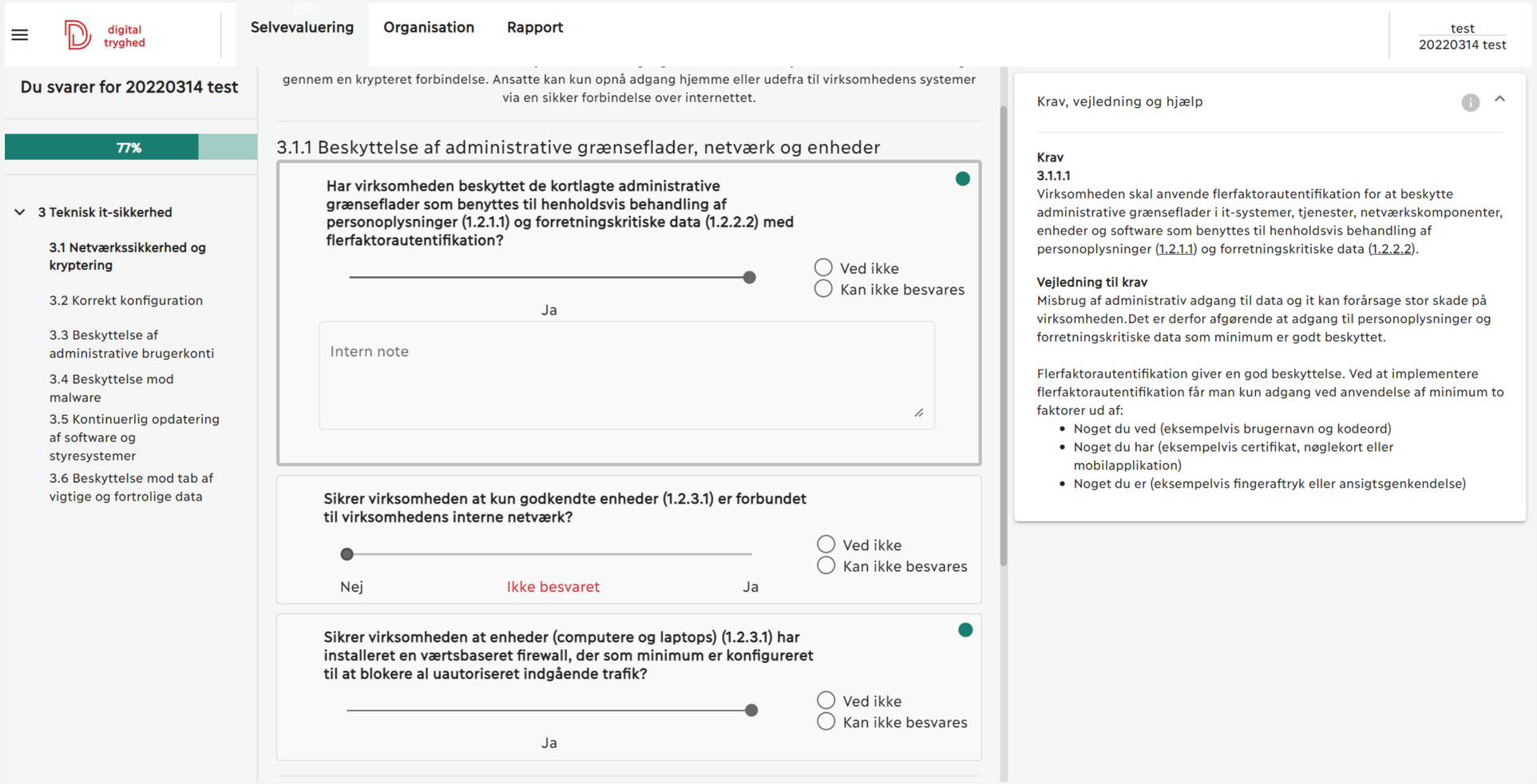
Kilde: https://d-maerket.dk/proces/

D-mærkets selvevalueringsværktøj



Kilde: https://digital.d-maerket.dk/

D-mærkets selvevalueringsværktøj



Kilde: https://digital.d-maerket.dk/

Find hjælp til at dokumentere D-mærkets krav

Det kan være svært at vurdere, hvornår nok er nok, når virksomheden skal dokumentere, at den lever op til D-mærkets krav. I D-mærkets oversigt over hjælpemidler, kan din virksomhed få overblik over, hvor der kan findes templates og værktøjer til at dokumentere D-mærkets krav. Oversigten hjælper virksomheder i processen henimod D-mærket. Bliv klogere på, hvad oversigten indeholder og hvordan din virksomhed kan bruge den.

Kilde: Find hjælp til at dokumentere D-mærkets krav | D-mærket (d-maerket.dk)

FÅ HJÆLP TIL AT BLIVE D-MÆRKET

Søg 50.000,- til rådgivning gennem SMV:Digital

Kilde: Få hjælp til at blive D-mærket: Søg 50.000 kr. til rådgivning gennem SMV:Digital | D-mærket (d-maerket.dk)

Betaling

	Gruppe I	Gruppe II	Gruppe III	Gruppe IV	Gruppe IV+
	0-9 ansatte	10-49 ansatte	50-249 ansatte	250-999 ansatte	>1000 ansatte
Pris for tilsyn	**DKK 2.800**	**DKK 8.400**	**DKK 21.000**	**DKK 52.250**	**Afhænger af størrelse**

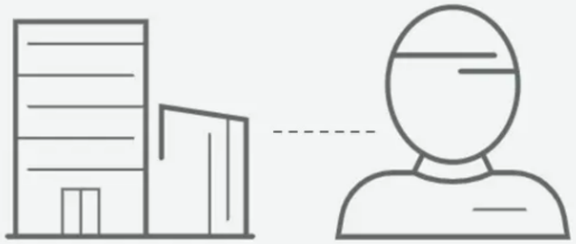
Undtagelser	**Max pris**	**Rabat**
Hvis under 10 ansatte, men tilhører virksomhedsgruppe III	DKK 8.400	-60%
Under 50 ansatte, men tilhører virksomhedsgruppe III	DKK 12.600	-40%

Kilde: https://d-maerket.dk/priser/

5

Tilsyn og kontrol

Tilsyn fra D-mærket foregår i tæt dialog med virksomheden



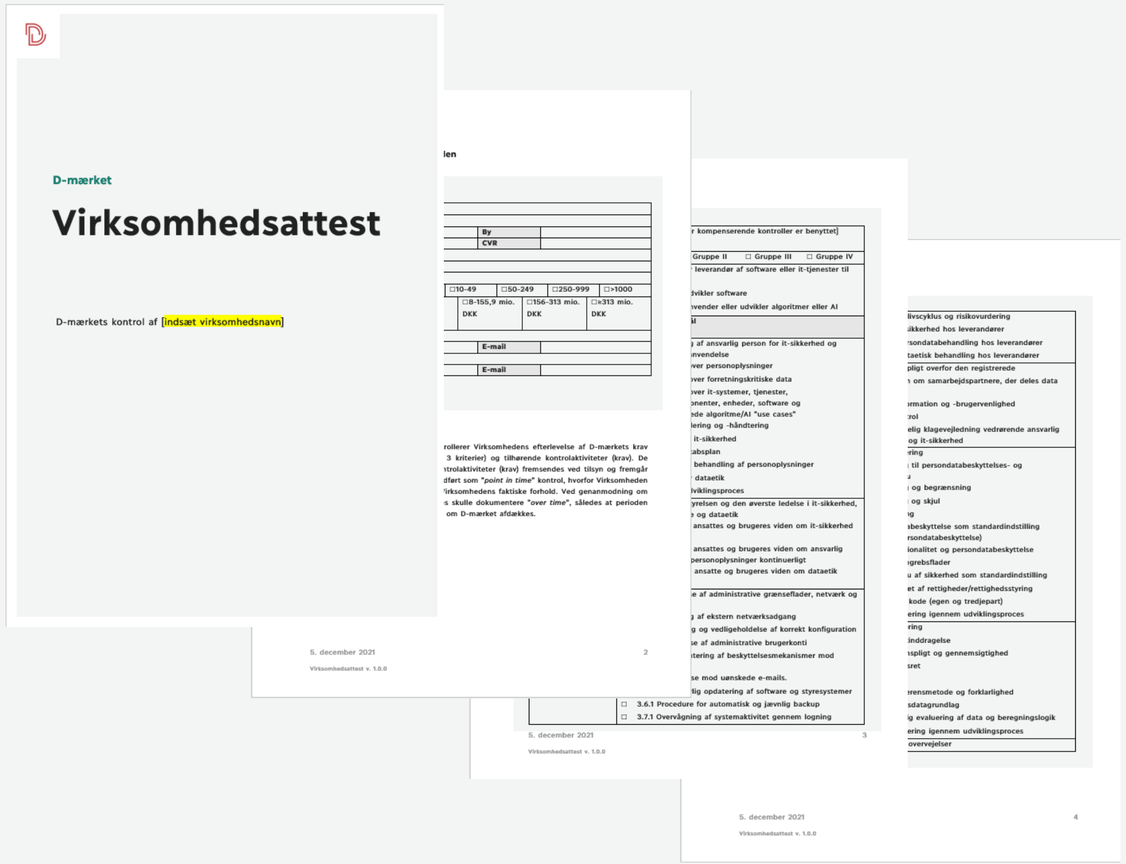
D-mærket fører tilsyn med, om virksomheden lever op til og kan dokumentere de besvarelser, den har angivet i D-mærkets selvevalueringsværktøj. Når virksomheden har besvaret de tildelte kriterier og krav med et "ja", kan den søge om tilsyn med henblik på at få tildelt D-mærket. Tilsyn fra D-mærket foregår i tæt dialog med virksomheden, og udføres altid af minimum to auditors. Det sikrer objektivitet og kvalitet.

Kilde: Tilsyn fra D-mærket foregår i tæt dialog med virksomheden | D-mærket (d-maerket.dk)

5

Tilsyn og kontrol

Kontrolrapport og virksomhedsattest



D-mærket

Virksomhedsattest

D-mærkets kontrol af [indsæt virksomhedsnavn]

5. december 2021

Virksomhedsattest v. 1.0.0

2

By	
CVR	

□10-49	□50-249	□250-999	□>1000
□8-155,9 mio. DKK	□156-313 mio. DKK	□≥313 mio. DKK	

E-mail	
E-mail	

5. december 2021

Virksomhedsattest v. 1.0.0

3

	□ 3.6.1 Procedure for automatisk og jævnlig backup		
	□ 3.7.1 Overvågning af systemaktivitet gennem logning		

5. december 2021

Virksomhedsattest v. 1.0.0

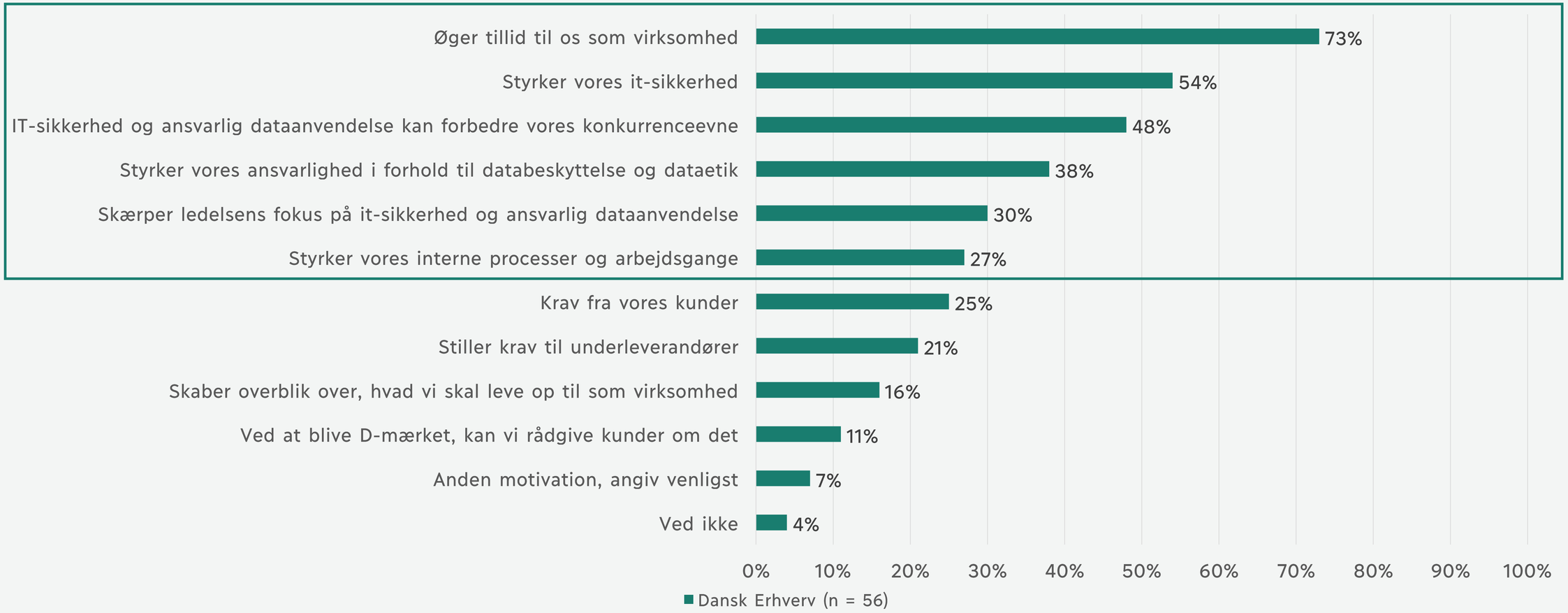
4

Kilde: D-mærket

Kapitel 4

Hvad får din virksomhed ud af D-mærket?

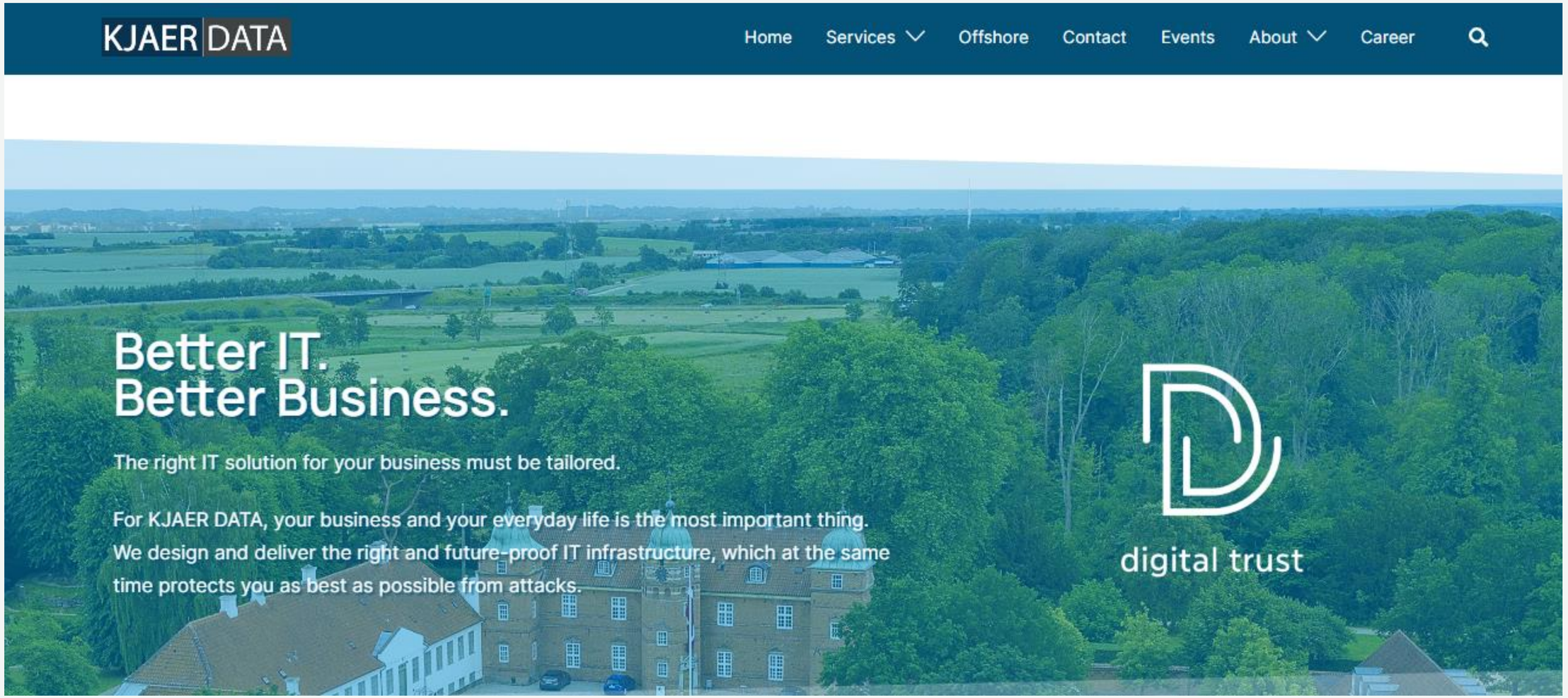
Motiver for at blive D-mærket



Note: Stillet til virksomheder der allerede deltager i D-mærket eller virksomheder med kendskab som vurderer, at det er sandsynligt, at de fremadrettet vil søge om at blive D-mærket. Det har være muligt at angive flere svarmuligheder, hvorfor andelene ikke summerer til 100

Kilde: Analyse af barrierer for at blive certificeret med D-mærket, Præsentation fra Pluss til D-mærkets styregruppe den 14. juni 2022

D-mærket er også et brand- og marketingværktøj



Kilde: Front Page - KJAER-DATA

”Vi forventer, at D-mærket bliver en blåstempling af virksomheders it-sikkerhed”

Mandag d. 03. jan. 2022

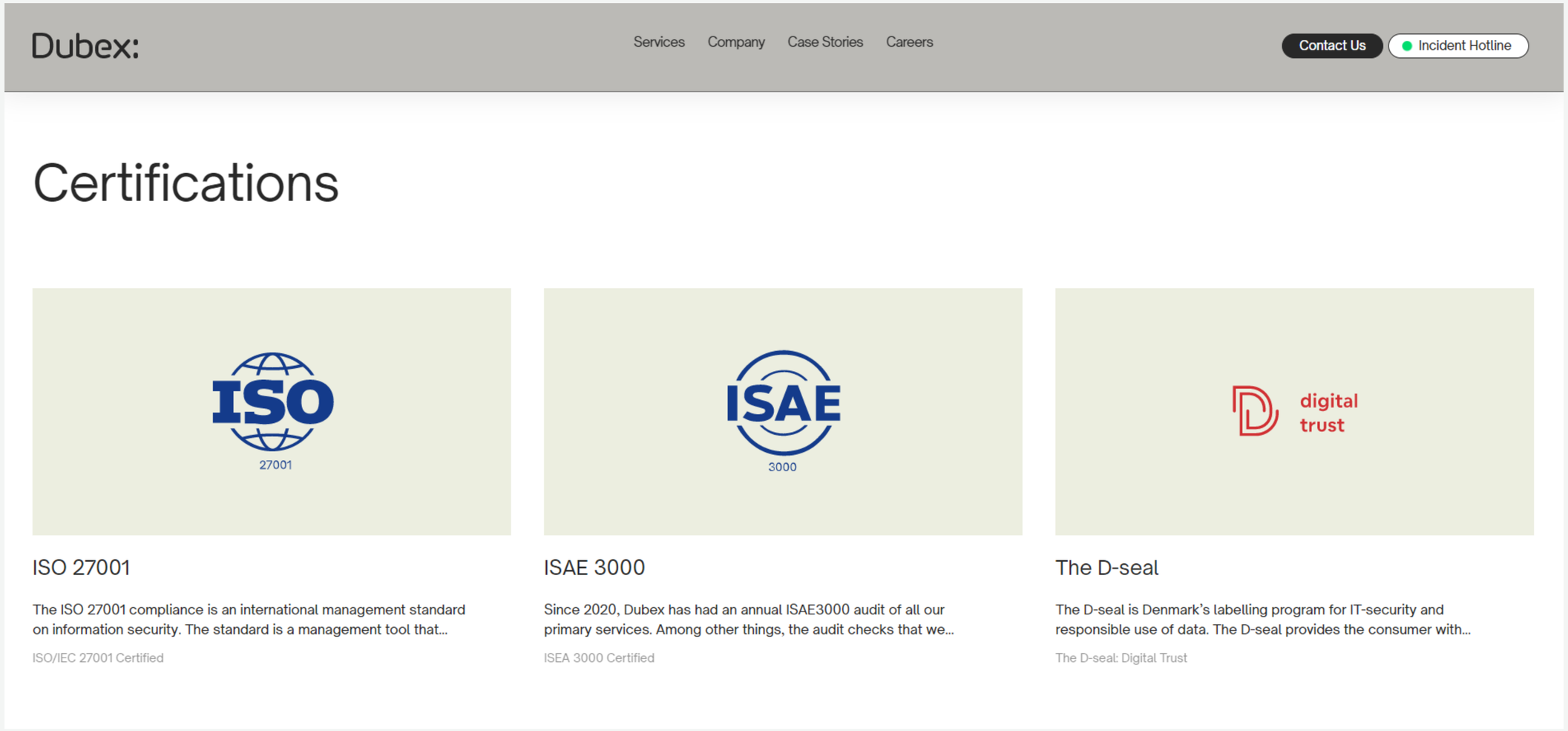
Dubex A/S leverer serviceydelser inden for cyber- og informationssikkerhed. Derudover driver Dubex et danskbasereret, døgnbemandet Cyber Defence Center, som overvåger kunders sikkerhed, og hjælper dem med Incident Response og Forensics, hvis de bliver udsat for cyberangreb.

Dubex A/S er hjemmevant i certificeringer og har i over 10 år været ISO 27001-certificeret inden for informationssikkerhed i forbindelse med udvikling, levering og servicering af løsninger og ydelser indenfor it-sikkerhed. Dubex A/S er en af de første virksomheder, der har fået D-mærket, og selvom virksomheden allerede har stor erfaring med ISO 27001, så har alle certificeringsprocesser værdi og bringer noget nyt med sig. Og hos Dubex A/S var det særligt D-mærkets krav inden for dataetik, der skabte nye overvejelser og krav til dokumentation.

CTO i Dubex A/S, Jacob Herbst fortæller, hvilke tiltag de igangsatte i processen henimod D-mærket, hvad de forventer at få ud af det og hvorfor certificeringsprocesser er gavnlige for alle virksomheder.

Kilde: ”Vi forventer, at D-mærket bliver en blåstempling af virksomheders it-sikkerhed” | D-mærket (d-maerket.dk)

D-mærket komplementerer andre certificeringer



Source: Certifications and compliance – Dubex

ViSikrer er meget bedre stillet nu, da viden om virksomhedens it ikke kun findes i Johnnys hoved

Torsdag d. 25. aug. 2022

Rådgivning og ydelser indenfor sikringsområdet for havne- og havnefaciliteter

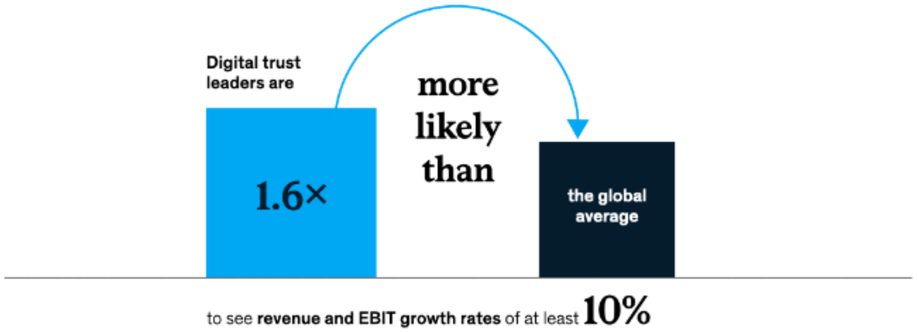
ViSikrer ApS' tildelingsbevis

I marts 2022 holdt D-mærkets direktør oplæg, om at skabe forretningsværdi gennem fokus på dataansvarlighed i Vordingborg. Her deltog Johnny Dalgaard, partner i ViSikrer ApS. Han var egentlig mest kommet for at networke, men da oplægget var slut, havde Johnny taget en beslutning: ViSikrer skulle D-mærkes og deres kunder skulle høre om D-mærkets fordele. D-mærket var nemlig både en god anledning til at gennemgå virksomhedens it-sikkerhed og nedskrive procedurer, men det åbnede også en ladeport af muligheder, for at levere ekstraydelser til ViSikrers kunder.

VISikrer ApS er en tomandsvirksomhed fra Guldborg på Lolland-Falster. Virksomheden arbejder med rådgivning og tilbyder en bred vifte af ydelser indenfor sikringsområdet for havne- og havnefaciliteter, bl.a. sårbarhedsvurderinger og sikringsplaner. Johnny Dahlgaard fortæller nedenfor, om ViSikrers motivation, processen henimod D-mærket og hvilke fordele virksomheden forventer.

Kilde: Case - ViSikrer er meget bedre stillet nu | D-mærket (d-maerket.dk)

McKinsey: ”Digital trust leaders lose less and grow more”



The survey results suggest that delivering on digital trust could provide significant benefits beyond satisfying consumer expectations. Leaders in digital trust are more likely to see revenue and EBIT growth of at least 10 percent annually.

Digital-trust leaders lose less and grow more

Digital-trust leaders are defined as those companies with employees who follow codified data, AI, and general ethics policies and that engage in at least half of the best practices for AI, data, and cybersecurity that we asked about. These companies are outperforming their peers both in loss prevention and business growth.

Kilde: Digital trust: Why it matters for businesses | McKinsey

digital tryghed

www.d-mærket.dk

D-mærket/D-seal

@Dmaerket

DANSK ERHVERV

DI

SMVdanmark

FORBRUGERRÅDET TÆNK

H. C. Andersens Boulevard 18, 1553 København V • Telefon: +45 33 77 33 77 • kontakt@d-maerket.dk